# HOW TO: Proof of Concept

# One-Arm (Sniffer) Mode

**Fortinet LATAM SE Team**

**Version 1.9**

**May 2014**

## DOCUMENT CHANGES LOG

| Version | Author | Date | Change(s) |
|---|---|---|---|
| 1.0 | Marcelo Mayorga | Sep 5, 2013 | Main document template, FortiGate configuration |
| 1.1 | Marcelo Mayorga | Sep 9, 2013 | Changed Template, FortiAnalyzer configuration |
| 1.2 | Marcelo Mayorga | Sep 22, 2013 | Report Generation |
| | Vadin Corrales | | Fixed errors and added comments |
| 1.3 | Marcelo Mayorga | Nov 7, 2013 | Added reference |
| | Vadin Corrales | | Fixed errors and added comments |
| 1.4 | Marcelo Mayorga | Dec 11, 2013 | Updated document to FortiAnalyzer 5.0.5 |
| | José Luis Laguna Merino | | Added check-list section |
| | Matteo Arrigoni | | Content fixes |
| 1.5 | Marcelo Mayorga | Dec 13, 2013 | Changed on report generation section, Added customer report import “Application and Risk Analysis – One Arm” |
| | Martin Hoz | | Added disclaimer and some content correction |
| 1.6 | Marcelo Mayorga | Dec 18, 2013 | Fixed minor changes |
| | Martin Hoz | | Fixed errors, added content on disclaimer, benefits and drawbacks and others |
| 1.7 | Marcelo Mayorga | Dec 21, 2013 | Changed IPS configuration (enable all signatures) |
| | | | Updated document for FortiOS 5.0.5 |
| | | | Simplified ARA One Arm datasetsconf |
| | | | Added sample report |
| 1.8 | José Luis Laguna Merino | Apr 17, 2014 | Added FortiAnalyzer best practice regarding disk quota. |
| 1.9 | Michel Barbosa | May 15, 2014 | Added presentations tips and minor changes |

## CONTACT

For comments or suggestions about this document, please contact document coordinator Marcelo Mayorga (mmayorga@fortinet.com)

## DISCLAIMER

This documents is intended for Fortinet engineers with experience on information security, networking and at least one year configuring FortiGate and FortiAnalyzer, using version 5 of their respective operating systems.

This document is NOT intended for end users or people not used to install and/or operate network security technology.

Fortinet, its employees and affiliates are not responsible for any service affection or impact that could be generated while doing any activity described in this document.

# INTRODUCTION

## DOCUMENT GOAL

The goal of this document is to provide a guideline on how to do a Proof of Concept (POC) and show how a network might be protected, without the necessity of building a complete working vehicle for that purpose. This is achieved by means of FortiGate capability of acting as a one-arm device in the network.

## PREPARE YOURSELF

Similar to what happens in an actual product deployment, the success of a Proof of Concept is extremely tied to a proper and responsible planning. Before doing any action, make sure you:

1) Call the customer, gather and set expectations
2) Gather and document information, credentials, IP address schemes, etc.
3) Products are registered and have a valid contract (See: “Registering your unit” below).
4) Make sure paperwork and administrative tasks have been done. Remember some companies require approval in order to allow gear to get into their premises or insert it into their network.
5) Last but not least, make sure you know the entire process. Try the whole procedure at least once on a controlled environment (may be your own company network). The last thing you want to do is to look doubtful in front of a potential customer!

## SNIFFER MODE / ONE-ARM / SPAN MODE – BENEFITS AND DRAWBACKS

Before getting into the technical stuff is important to understand that deploying a FortiGate in a one-arm topology has benefits and drawbacks.

**NOTE**

On this document the terms *sniffer*, *one-arm* and *span* modes are used interchangeably

Benefits:

- Non-intrusive: Does not require mayor changes nor will affect network performance.
- Provides real-time visibility of customer's traffic
- Allows a customer (prospect) to familiarize with Fortinet's GUI without the associated risk of interfering with production traffic.

Drawbacks:

- Not valid for sizing or performance measurement: Processing traffic in sniffer mode does not demand the same kind and amount of resources as it takes doing inline inspection.
- It does not provide (and shouldn't be positioned as) security protection. The focus is on visibility
- Some traffic might not be caught and some FortiGate inspection features won't work on this mode.
- SSL Inspection is not supported in sniffer mode.

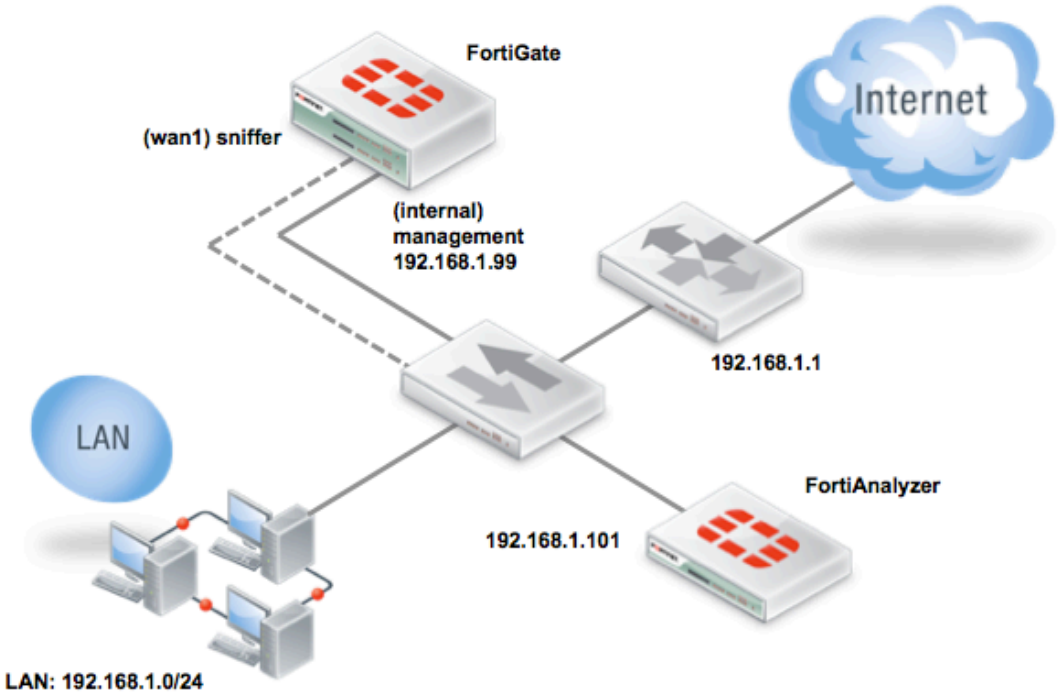
## REQUIRED GEAR AND VERSIONS USED

For this document, the following versions were used.

- FortiGate: This document was created using FortiOS 5.0.5 (build0252).
- FortiAnalyzer: This document was created using FortiOS 5.0.5 (build0266).

While the hardware models used on this document are a FortiGate-60C and a FortiAnalyzer VM, It is recommended to properly size the right hardware. If in doubt, size like if the FortiGate were going to do full inline inspection and the FortiAnalyzer were to receive full logging.

## NETWORK TOPOLOGY



## REGISTERING YOUR UNIT

Remember that your FortiGate unit must be registered within Fortinet Support system in order to be able to access FortiGuard services and thus updating its security databases (AV, IPS, Applications, etc.).

For a detailed guide on how to register a Fortinet product, read the following document: https://support.fortinet.com/Download/RegistrationGuide.pdf

## TYPOGRAPHIC CONVENTIONS

Whenever you see this:

```
CLI
```

It means the following steps can be done using the Command Line Interface

Whenever you see this:

```
GUI
```

It means the following steps can be done using the Graphical User Interface

## HANDS-ON: FORTIGATE CONFIGURATION

This document has been created starting from a factory default configuration. If you're not an experienced user we recommend you to restore your FortiGate to defaults before moving on. Of course, a previous backup might be wise.

1. Connect to your FortiGate either through CLI (SSH/Telnet/Console) or using the embedded CLI Console widget in FortiGate's GUI
2. Execute:

**CLI**

```
# exec factoryreset
This operation will reset the system to factory default!
Do you want to continue? (y/n)y
```

### DISABLE DHCP SERVER

If you're starting from a factory configuration is probable that you have a DHCP server configured. Make sure you delete it in order to avoid any conflict with other DHCP servers in the network.

**CLI**

```
FGT60C # config system dhcp server

FGT60C(server) # show
config system dhcp server
    edit 1
        set default-gateway 192.168.1.99
        set dns-service default
        set interface "internal"
```

```
            config ip-range
                edit 1
                    set end-ip 192.168.1.254
                    set start-ip 192.168.1.100
                next
            end
        set netmask 255.255.255.0
    next
end

FGT60C3G12047125 (server) # delete 1
```

Repeat “delete” operation for any entry listed.

## CONFIGURING MANAGEMENT INTERFACES

With default configuration, login to the FortiGate and configure one interface to be used for management purpose.

**NOTE**

Default management interface will depend on FortiGate model. If you don’t know which interface to use, take a look to corresponding QuickStart Guide: http://docs.fortinet.com/

Default management IP address: 192.168.1.99

Login credentials: admin/<blank password>

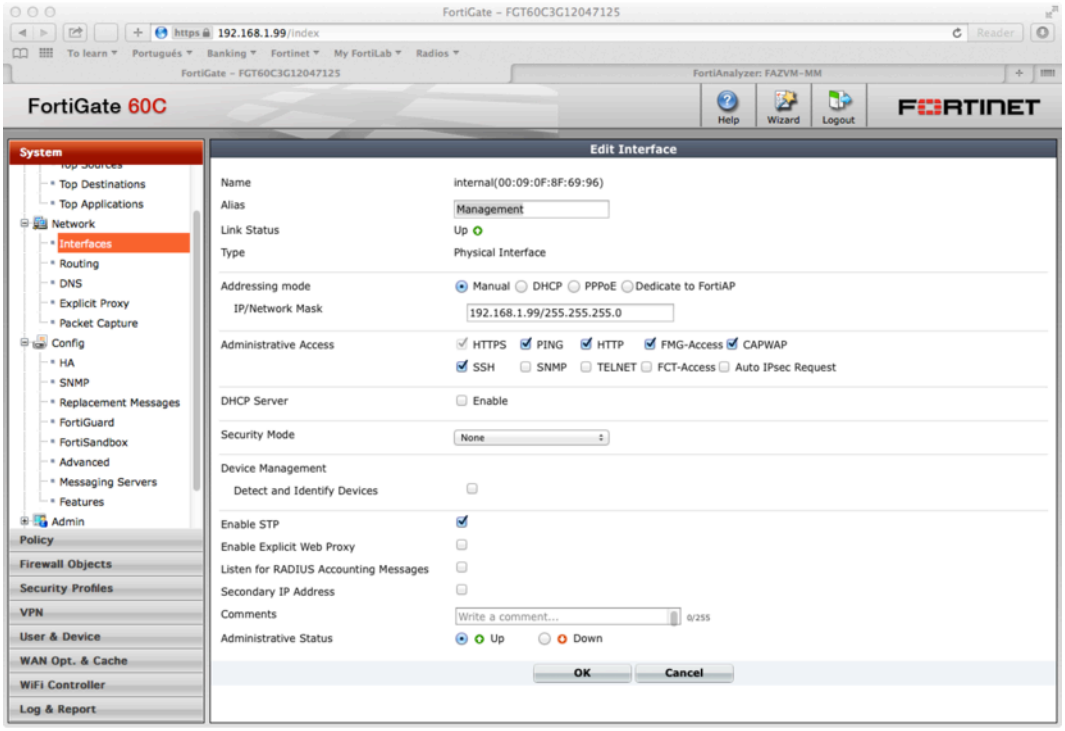
**CLI**

```
config system interface
    edit "internal"
        set vdom "root"
        set ip 192.168.1.99 255.255.255.0
        set allowaccess ping https ssh http fgfm capwap
        set type physical
        set alias "Management"
        set snmp-index 1
```

```
    next
end
```

**GUI**

1. Go to System → Network → Interfaces
2. Select appropriate management interface.
3. Configure Alias as “Management” (optional)
4. Configure IP/Mask
5. Make sure DHCP checkmark is disabled
6. OK



Remember that your FortiGate must reach FortiGuard servers in order to do Web Filtering, update IPS/AV databases and engines.

Configure DNS Servers and routing in order to reach the Internet.

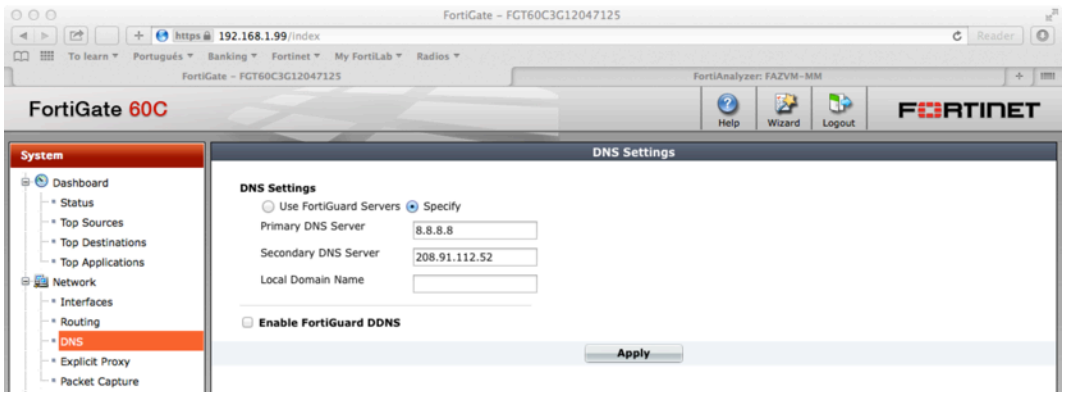
## CONFIGURE DNS SERVERS:

**CLI**

```
config system dns
    set primary 8.8.8.8
    set secondary 208.91.112.52
end
```

**GUI**

1. Go to System → Network → DNS
2. Configure Primary and Secondary DNS
3. Apply



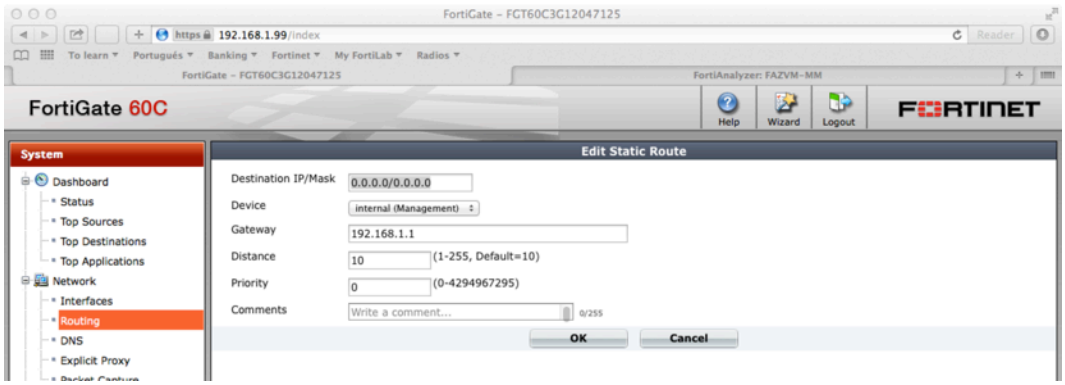
## CONFIGURE DEFAULT GATEWAY

**CLI**

```
config router static
    edit 0
        set device "internal"
        set gateway 192.168.1.1
    next
end
```

**GUI**

1. Go to System → Network → Routing
2. Under Static Routes: Create New




3. Add Gateway and outgoing Device (i.e. interface facing default gateway).
4. OK


## VERIFY ROUTING TABLE

**CLI**

```
# get router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

S*      0.0.0.0/0 [10/0] via 192.168.1.1, internal
C       192.168.1.0/24 is directly connected, internal
```

Verify you are able to reach an Internet host:

**CLI**

```
# exec ping www.yahoo.com
PING ds-fp3.wg1.b.yahoo.com (206.190.36.45): 56 data bytes
64 bytes from 206.190.36.45: icmp_seq=0 ttl=52 time=220.2 ms
64 bytes from 206.190.36.45: icmp_seq=1 ttl=52 time=230.0 ms
64 bytes from 206.190.36.45: icmp_seq=2 ttl=52 time=222.2 ms
64 bytes from 206.190.36.45: icmp_seq=3 ttl=52 time=238.3 ms
64 bytes from 206.190.36.45: icmp_seq=4 ttl=52 time=263.2 ms

--- ds-fp3.wg1.b.yahoo.com ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 220.2/234.7/263.2 ms
```

## UPDATE YOUR SECURITY SERVICES DATABASES

Once your unit has access to Internet is the right time to update your FortiGate's security services databases. Having up-to-date databases and engines is a key part of the Proof of Concept as this will improve catch-rates, performance and customer overall impression.

As first step you should configure Antivirus to use the "normal" database

**CLI**

```
config antivirus settings
    set default-db normal
end
```

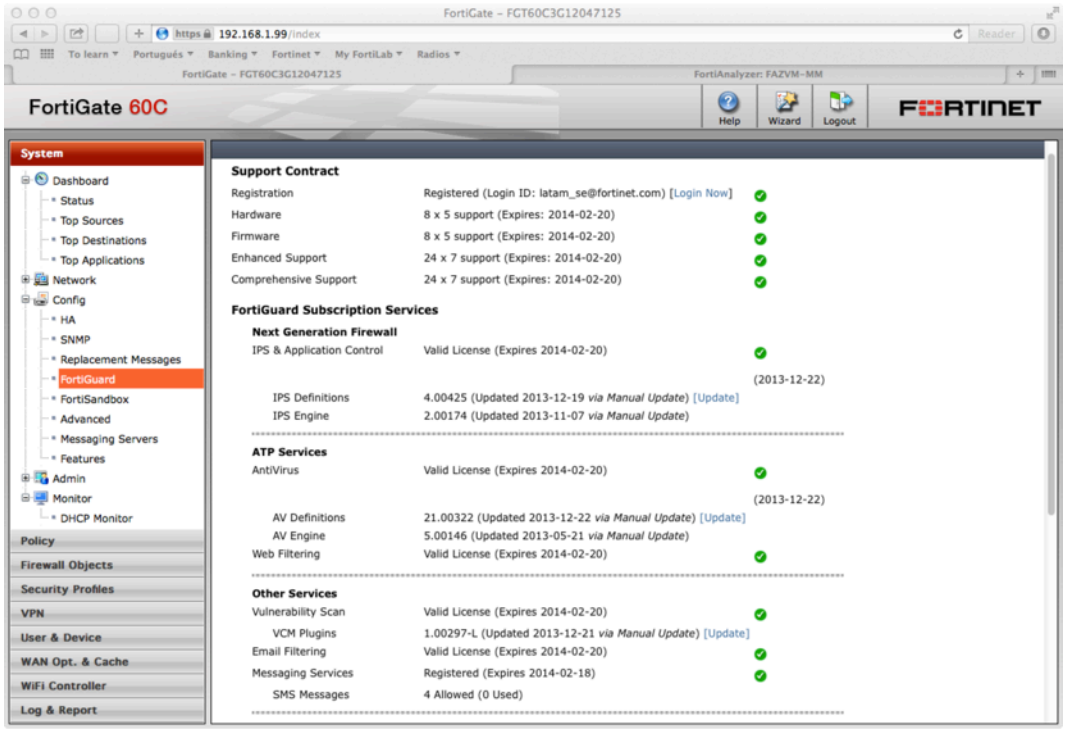
Update FortiGuard signatures and engines.

**CLI**

```
# exec update-now
```

**GUI**

1. Go to System → Config → FortiGuard
2. Expand the "AV & IPS Download Options" section and click on "Update Now"
3. Make sure FortiGuard Subscription Services appear with a green check mark at least for Antivirus, IPS & Application Control and Web Filtering




**NOTE**

By default, FortiGate uses port UDP/53 for communicating with the FortiGuard servers. It might be the case that a filtering device blocks this traffic for not being DNS (e.g. a DPI in the network). If that's the case, you have the option of using port UDP/8888

## CONFIGURE TRAFFIC INTERFACE (SNIFFER)

Configure the interface that is going to be wired to the SPAN/Mirror port in the switch.

Remember to delete any reference (policies, routes, etc.) to the interface before changing it to sniffer-mode.

**BEST PRACTICE TIP**

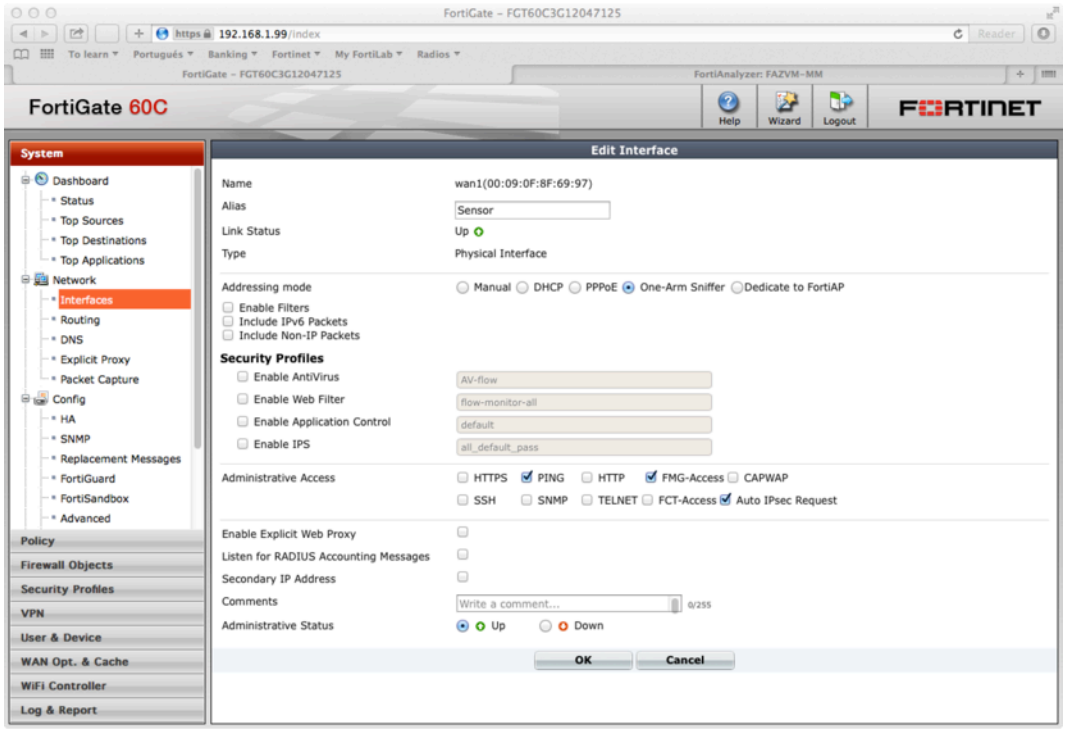
Using different interfaces for sniffing and management is recommended

**CLI**

```
config system interface
    edit "wan1"
        set vdom "root"
        set allowaccess ping
        set ips-sniffer-mode enable
        set type physical
        set alias "Sensor"
        set snmp-index 2
    next
end
```

**GUI**

1. Go to System → Network → Interfaces
2. Select appropriate traffic interface.
3. Configure Alias as “Sensor” (optional)
4. Select “One-Arm Sniffer” as Addressing Mode
5. OK




## CONFIGURE SECURITY PROFILES

In the next steps we will configure security profiles that will be used for traffic inspection. Be aware in that when running in sniffer mode only “flow-based” security profiles should be used, as there’s no possibility of proxies to intercept connection on this mode.

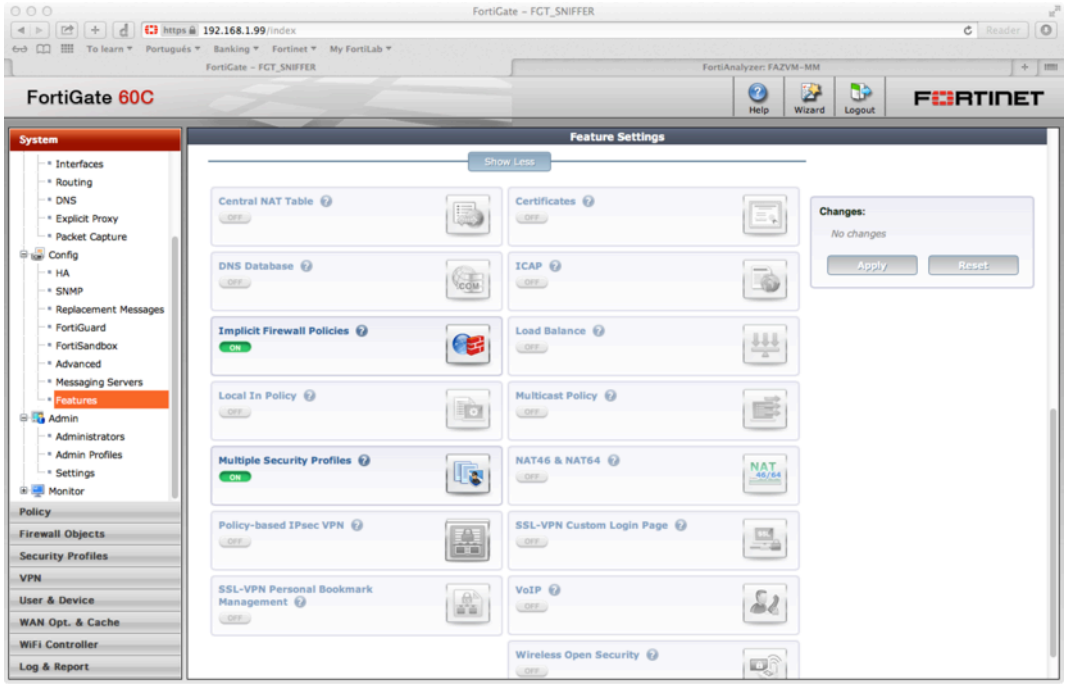
Enable multiple UTM profiles: If you’re using an entry level FortiGate you will probably have to enable the use of multiple UTM profiles, as by default just one profile per functionality can be configured.

**CLI**

```
config system global
    set gui-multiple-utm-profiles enable
end
```

**GUI**

1. Go to System → Config → Features
2. Click on “Show More”
3. Enable Multiple Security Profiles
4. Apply



For the purpose of this document we will use FortiGate pre-configured profiles and highlight in bold letter any alteration you need to do from the default.

**IMPORTANT**

Some of the settings on this section cannot be done through using the GUI. Once you finish your configuration check the profiles using CLI and make appropriate changes if necessary.

### Antivirus Profile:

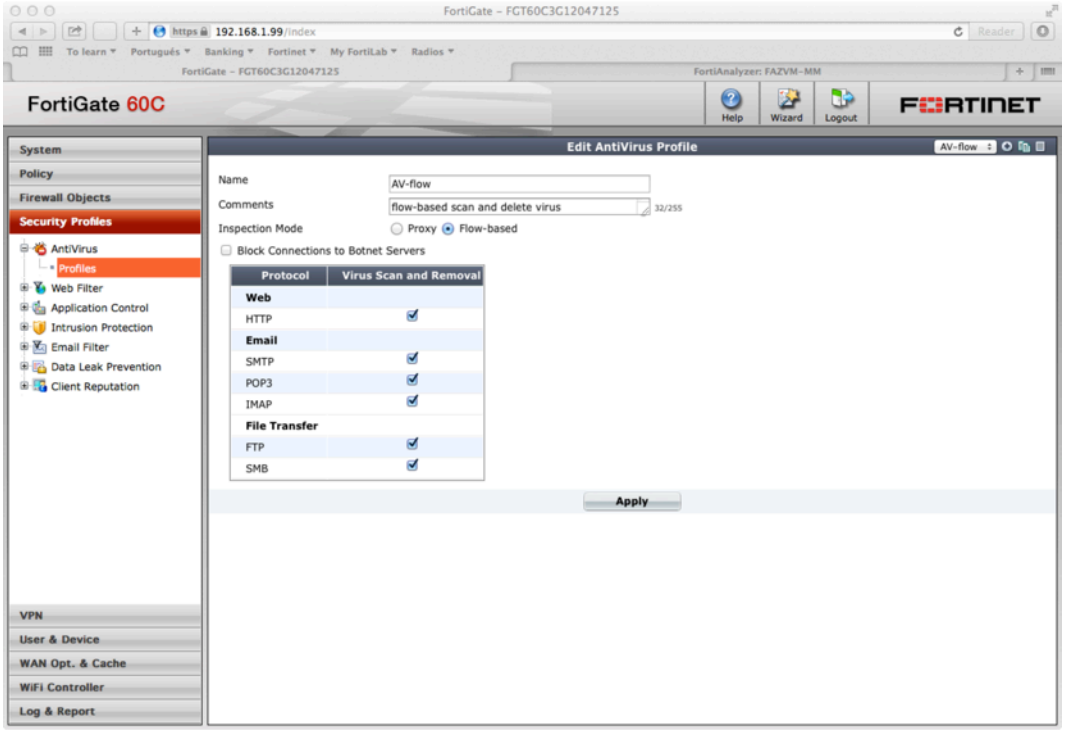
**CLI ONLY**

```
config antivirus profile
    edit "AV-flow"
        set comment "flow-based scan and delete virus"
        set inspection-mode flow-based
        set extended-utm-log enable
            config http
                set options scan
            end
            config ftp
                set options scan
            end
            config imap
                set options scan
            end
            config pop3
                set options scan
            end
            config smtp
                set options scan
            end
            config nntp
                set options scan
            end
            config im
                set options scan
            end
            config smb
                set options scan
```

```
            end
        set av-virus-log enable
        set av-block-log disable
    next
end
```

**GUI**

1. Go to Security Profiles → Antivirus → Profiles
2. Select AV-flow
3. Enable “Virus Scan and Removal” for every protocol
4. Apply



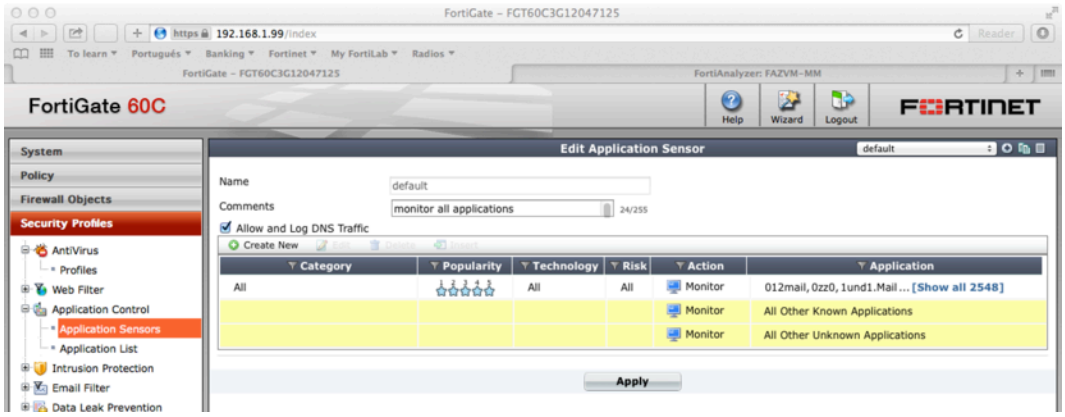
## Configure Application Control sensor:

**CLI ONLY**

```
config application list
    edit "default"
        set comment "monitor all applications"
        set extended-utm-log enable
        set other-application-log enable
        set log enable
        set unknown-application-log enable
            config entries
                edit 1
                    set action pass
                next
            end
    next
end
```

**GUI**

1. Go to Security Profiles → Application Control → Application Sensors
2. Select “default”
3. Apply



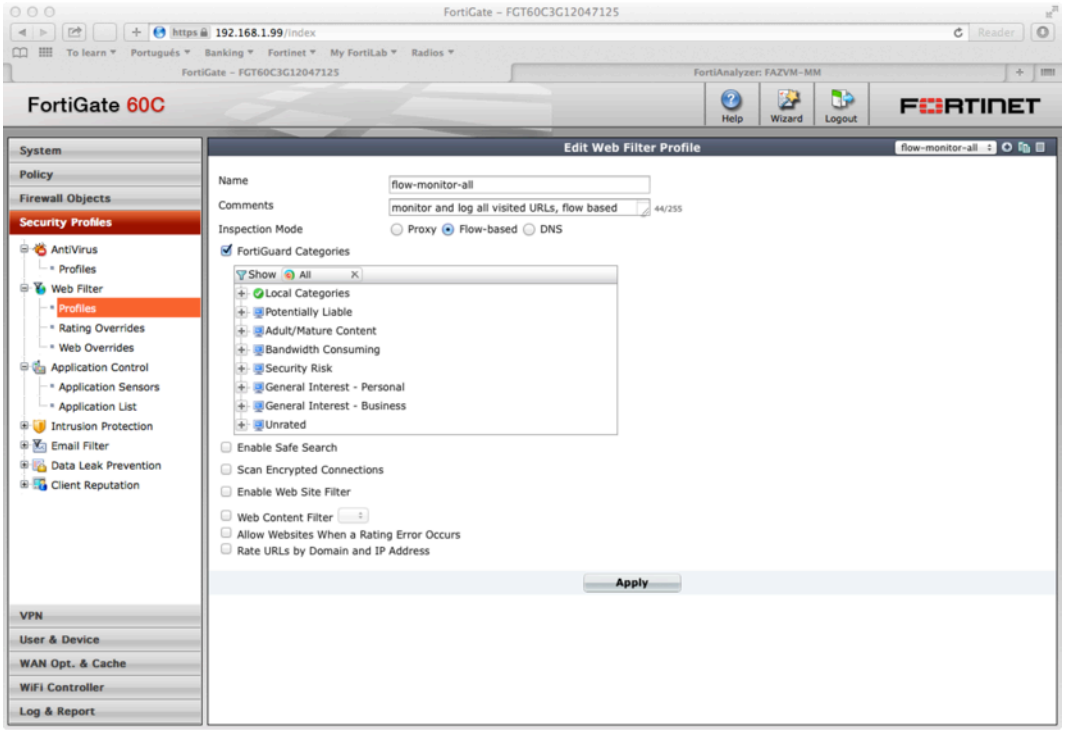
## Configure Web Filtering profile:

**CLI ONLY**

```
config webfilter profile
    edit "flow-monitor-all"
        set comment "monitor and log all visited URLs, flow based"
        set extended-utm-log enable
        set inspection-mode flow-based
        set options https-url-scan
            config ftgd-wf
                unset options
                unset exempt-ssl
                    config filters
                        edit 1
                            set category 1
                        next
                            (… other categories the same …)
                        next
                          edit 79
                        next
                    end
            end
        set log-all-url enable
        set web-content-log disable
        set web-filter-activex-log disable
        set web-filter-command-block-log disable
        set web-filter-cookie-log disable
        set web-filter-applet-log disable
        set web-filter-jscript-log disable
        set web-filter-js-log disable
        set web-filter-vbs-log disable
        set web-filter-unknown-log disable
        set web-filter-referer-log disable
        set web-filter-cookie-removal-log disable
        set web-url-log disable
        set web-invalid-domain-log disable
        set web-ftgd-err-log disable
        set web-ftgd-quota-usage disable
    next
end
```

GUI

1. Go to Security Profiles → Web Filter → Profiles
2. Select “flow-monitor-all”
3. Apply



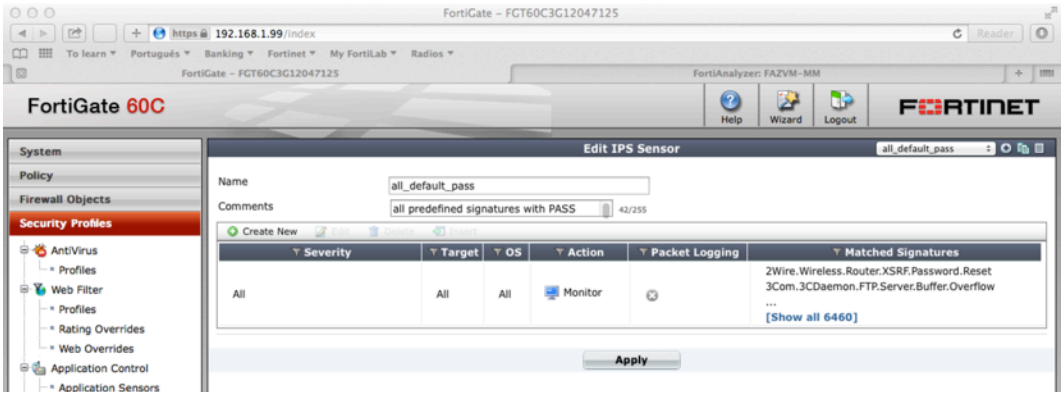
## Configure IPS Sensor:

**CLI**

```
config ips sensor
    edit "all_default_pass"
        set comment "all predefined signatures with PASS action"
            config entries
                edit 1
                    set action pass
                    set status enable
                next
            end
    next
end
```

**GUI**

1. Go to Security Profiles → Intrusion Prevention → IPS Sensor
2. Select “all_default_pass”
3. Apply

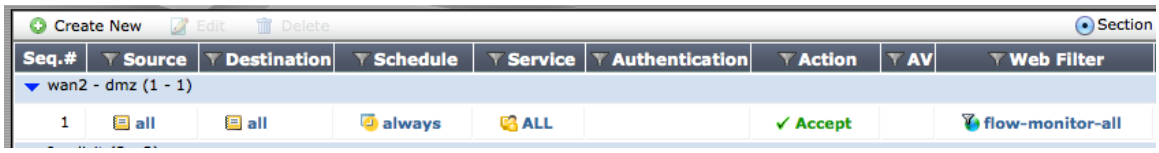


## CONFIGURE SNIFFER POLICY

Once the basic networking has been configured and has been defined security profiles, we just need to put both things together. Creating a special kind of policies known as “sniffer policies” does this.

**IMPORTANT TIP**

In case you want to generate reports containing URL Filtering categories make sure you create a policy containing a Web Filtering profile. FortiGuard rating won’t be enabled unless a policy containing a Web Filtering profile is defined.



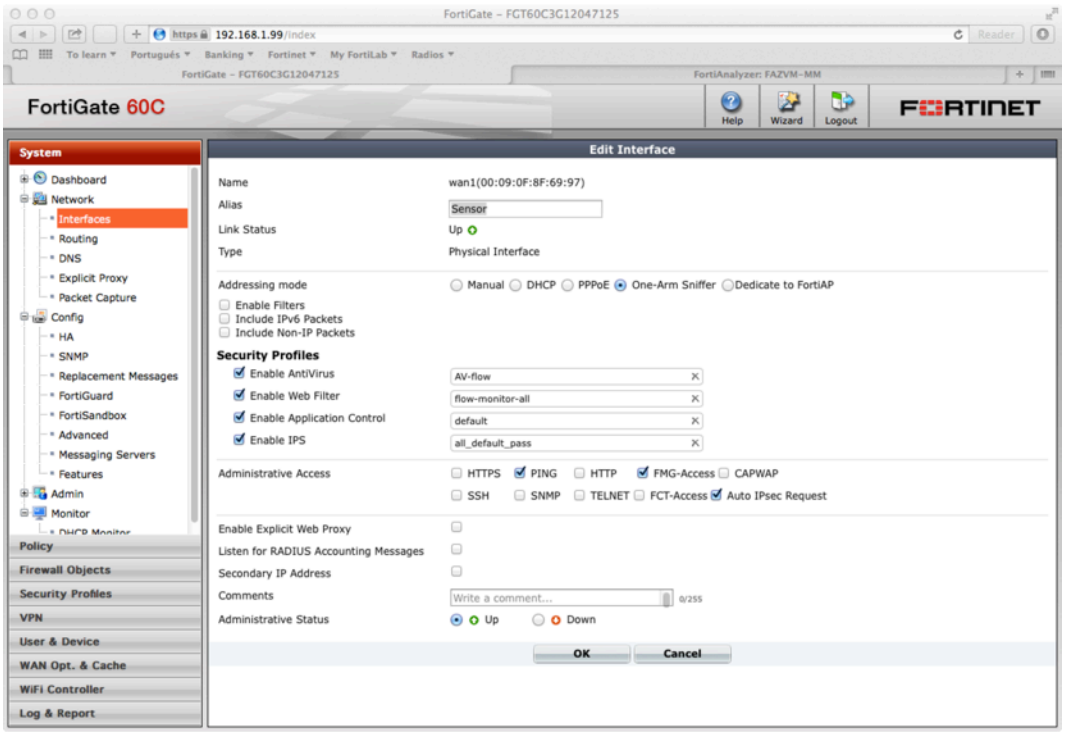

This tricky configuration has been identified and acknowledged for a future enhancement.

**CLI**

```
config firewall sniffer
    edit 0
        set logtraffic all
        set interface "wan1"
        set application-list-status enable
        set application-list "default"
        set ips-sensor-status enable
        set ips-sensor "all_default_pass"
        set av-profile-status enable
        set av-profile "AV-flow"
        set webfilter-profile-status enable
        set webfilter-profile "flow-monitor-all"
    next
end
```

**GUI**

1. Go to System → Network → Interfaces
2. Edit appropriate traffic interface.
3. Enable Security Profiles for Antivirus, Web Filter, Application Control and IPS, select recently configured profiles
4. OK



## HANDS-ON: FORTIANALYZER CONFIGURATION

In order to provide better visibility and full reporting we will integrate the FortiGate device with a FortiAnalyzer. Let's remember FortiAnalyzer is the security architecture component that allows for a more professional reporting, compared to the basic reporting done by the FortiGate.

### CONFIGURE FORTIGATE LOGGING TO FORTIANALYZER

**CLI**

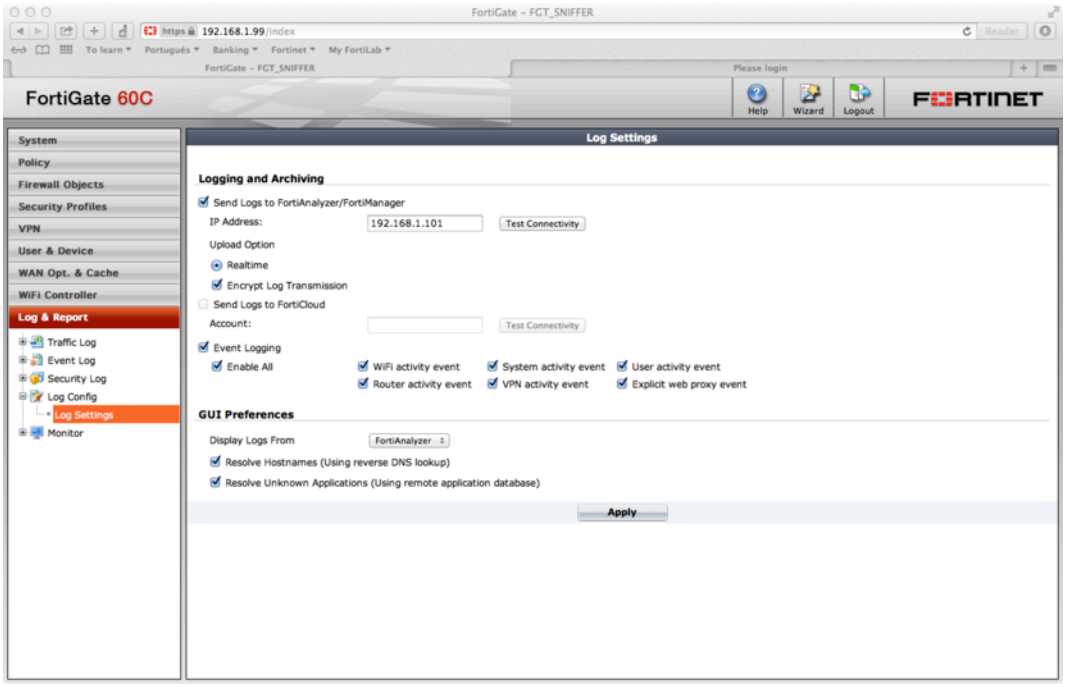
```
config log fortianalyzer setting
    set status enable
    set server 192.168.1.101
    set reliable enable
end
```

**GUI**

1. Go to Log & Report → Log Config → Log Settings
2. Enable "Send Logs to FortiAnalyzer/FortiManager"
3. Configure FortiAnalyzer's IP address
4. Apply

**NOTE**

When doing "Test Connectivity" you might get an error as the Device hasn't been accepted in the FortiAnalyzer yet.

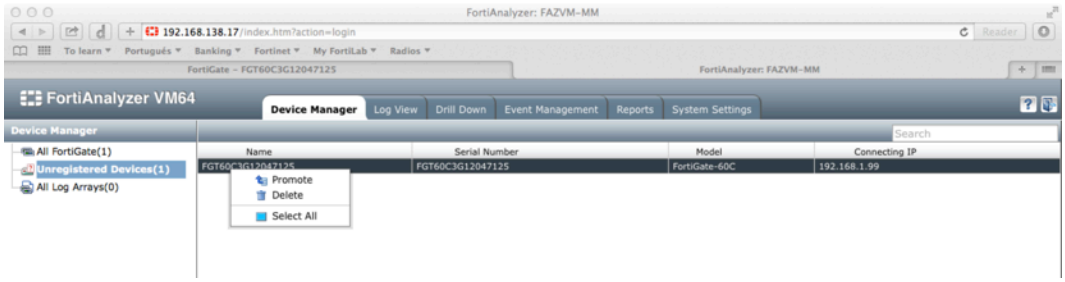



## CONFIGURE FORTIANALIZER FOR ACCEPTING FORTIGATE LOGGING

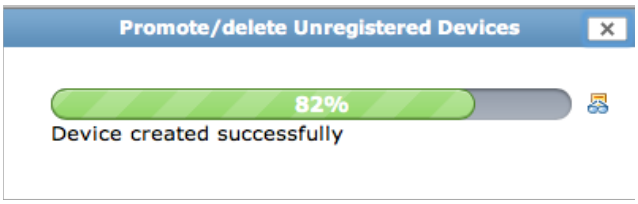
After configuring the FortiGate to send logs to FortiAnalyzer, you will need to accept the devices as logging resource. This is done from FortiAnalyzer's GUI.

**GUI**

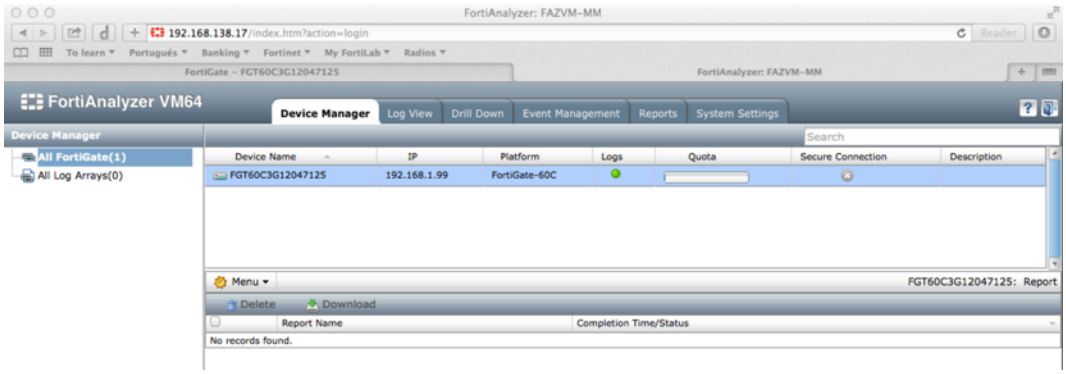
1. Login to FortiAnalyzer GUI using HTTP/S
2. Go to Device Manager tab
3. Look into "Unregistered Devices" list
4. Make sure you select the proper FortiGate in the list, right-click and select "Promote" from the list.




5. Wait until the process finish.




6. Verify your FortiGate appears listed as an accepted device.



**BEST PRACTICE TIP**

For POCs, make sure you modify FortiGate's quota and assign as much space as possible in the FortiAnalyer. You don't want to start overwriting logs. Right click over the FGT → Edit → Edit "Disk Log Quota" field

# HANDS-ON: PUTTING ALL TOGETHER – NETWORK CONFIGURATION

Once FortiGate and FortiAnalyzer have configured the last step would be setting up the network in order to send traffic to the FortiGate.

## CONFIGURE SWITCH

The FortiGate will receive traffic from a networking switch. First thing to understand is that because of this the FortiGate will only have visibility of traffic being redirected by this switch.

For the purpose of this Proof of Concept (POC) the recommendation would be to plug the FortiGate to the switch that receives all Internet facing traffic.

Configure SPAN/Mirror port:

This activity has to be done by company's networking specialists.

In order for FortiGate to get appropriate information, provides visibility and reporting, traffic in both directions should be copied/mirrored.

## VERIFY CONFIGURATION

Using network sniffer:

Once the switch has been configured everything is ready to start inspecting traffic. Before getting into graphics and reporting make sure you verify that FortiGate is actually receiving traffic. This can be done by running a TCP dump on sniffing configured interface:

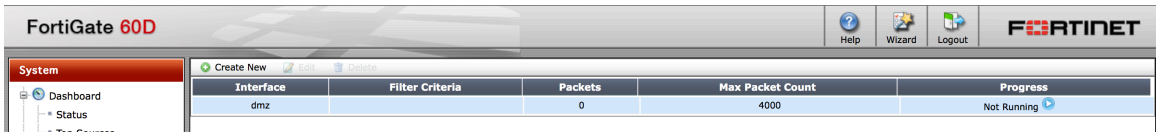
**CLI**

```
# diagnose sniffer packet wan1 '' 1
interfaces=[wan1]
filters=[]
0.592415 200.42.92.139.1935 -> 192.168.1.44.53307: psh 2596606569 ack
2829680690
0.592770 192.168.1.44.53307 -> 200.42.92.139.1935: ack 2596606587
…
…
…

66 packets received by filter
0 packets dropped by kernel
```

**GUI**

1. Go to System → Network → Packet Capture
2. Click “Create New”
3. Select the correct interface, OK
4. Start the capture on the blue play sign




5. Check if the packets are increasing
6. Stop the capture and analyze it on Wireshark to validate the traffic

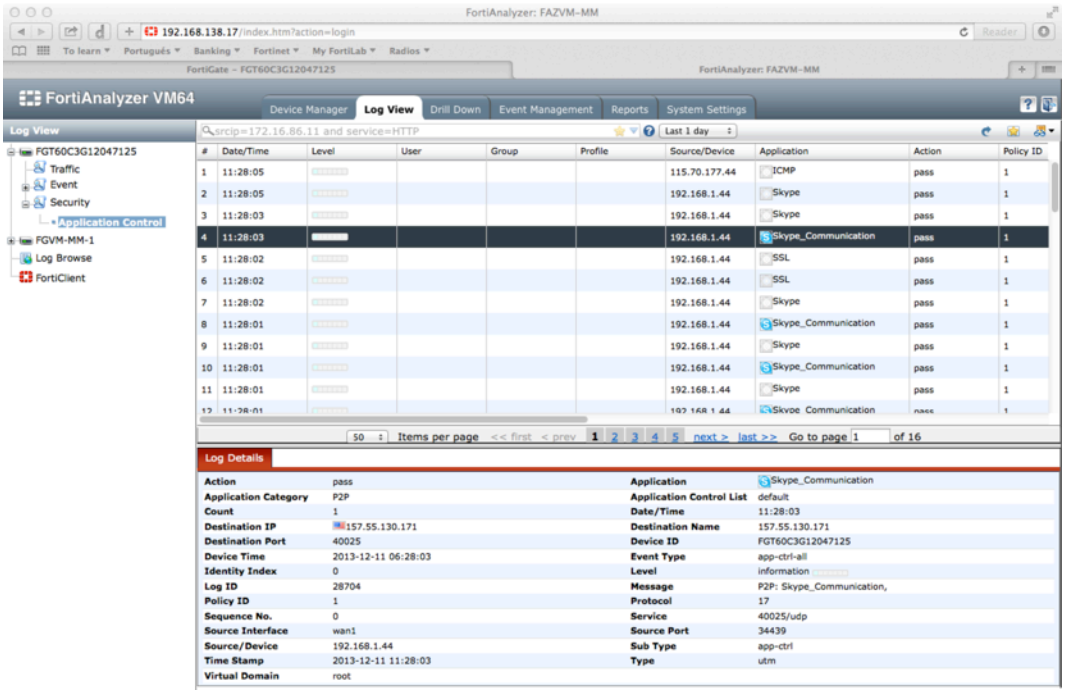
## HANS-ON: REVIEWING LOGS AND GENERATING REPORTS

Once your FortiGate and your networking device are configured you will be able to view logs, filter them and create reports. We will not go through the process of generating new reports but using a predefined one that has to be imported into the FortiAnalyzer.

### VIEWING LOS IN FORTIANALYZER

GUI

1. Login to FortiAnalyzer using HTTPS
2. Go to Log View tab
3. On left pane, select your FortiGate's name → Security → Application Control (other logs can be used for this example)
4. On right pane you should see a list of the log entries
5. Select any entry a see details below.



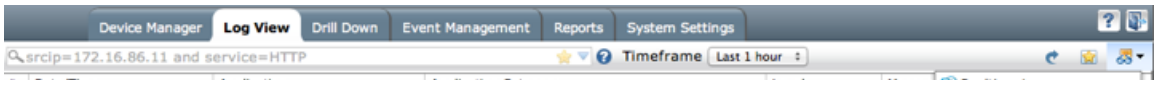

## Filtering logs in FortiAnalyzer

GUI

There're two ways of using filters with FortiAnalyzer 5.0.3:

1. Using the top filtering bar

   Top filtering bar allows you to use free text in combination with some tags in order to search for records in an easy and fast way



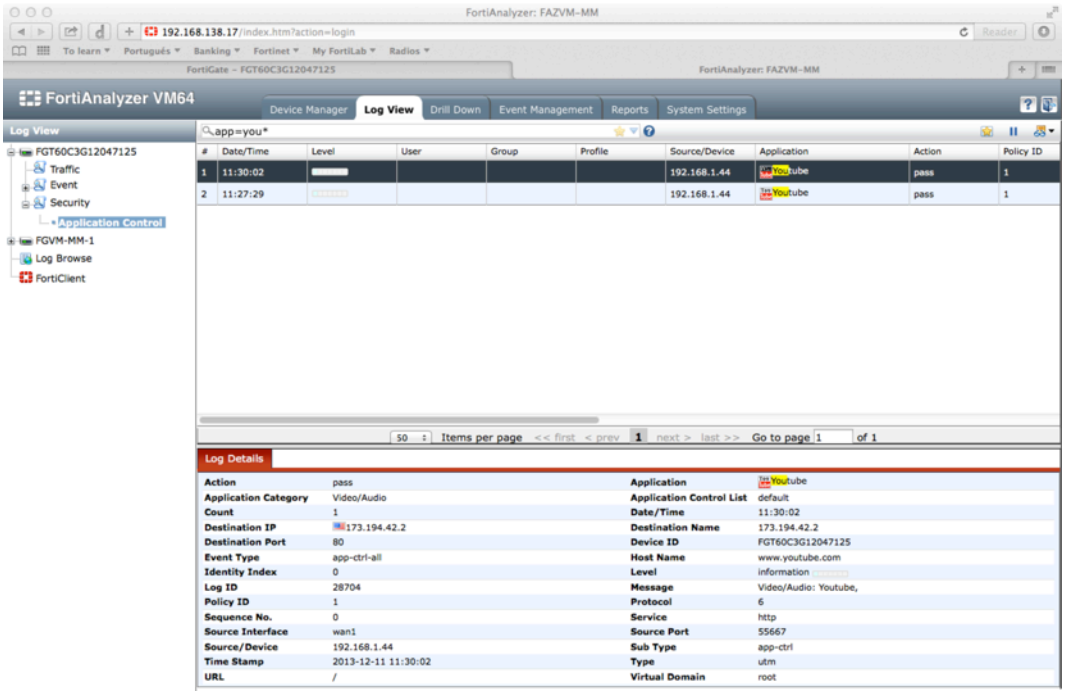

   Some example of searches you could do:

   - app=dns
   - app=youtu*

- apptype=vide*
- dstport=80 and srcip=192.168.1.*

**NOTE**

In order to ease your free text search, make sure you set “Case Insensitive Search” using View Options ( ) button.

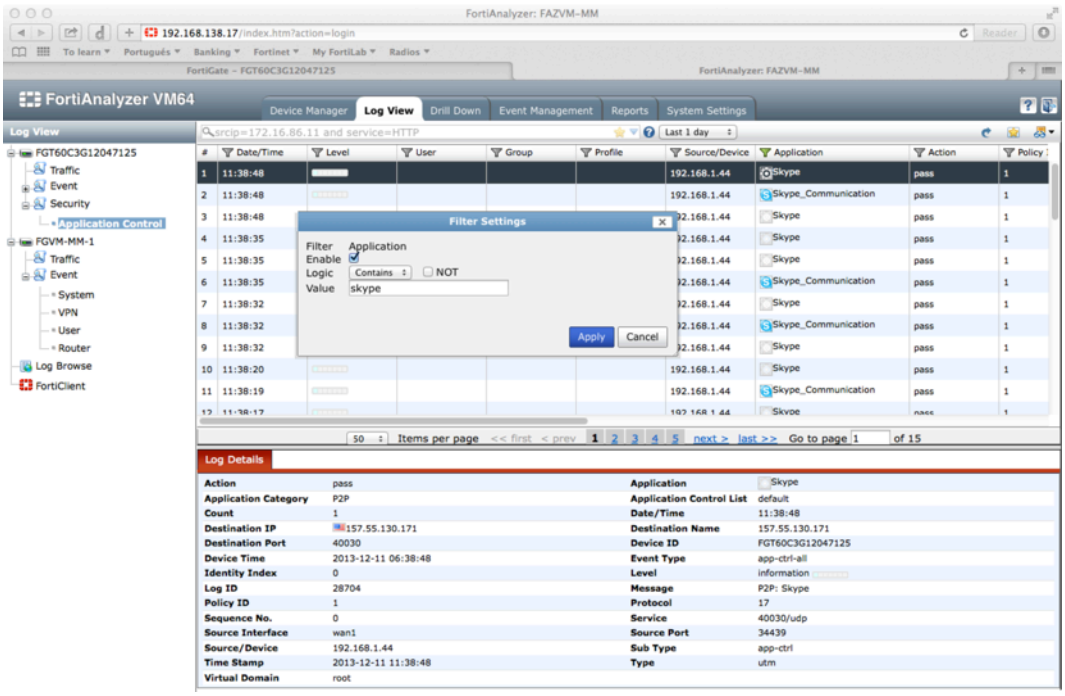



2. Using column filters

   Column filters the traditional way of filtering records by specifying the desired value on each column. When filters in more than one column are specified they are joined by a logical AND, so all filter has to be true in order for logs to appear.

**NOTE**

Column filters are not enabled by default. Click on View Options ( ) button and enable them.




Click on the filter icon over the column to specify the desire value for it.

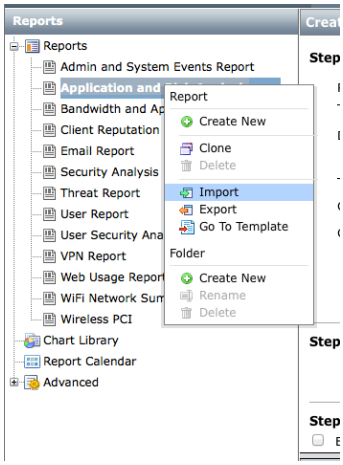
## GENERATING REPORTS IN FORTIANALYZER

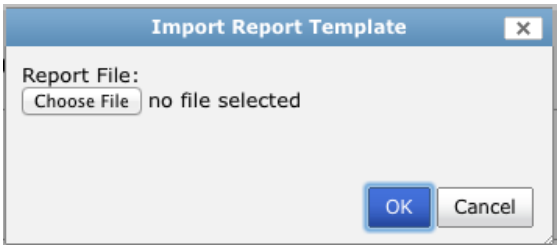
This section will show how to use and generate pre-configured reports. Generating new reports is outside the scope of this document.

For the sake of this POC we will use a special report created specifically for devices capturing traffic in one-arm mode, “Application and Risk Analysis – One Arm”.

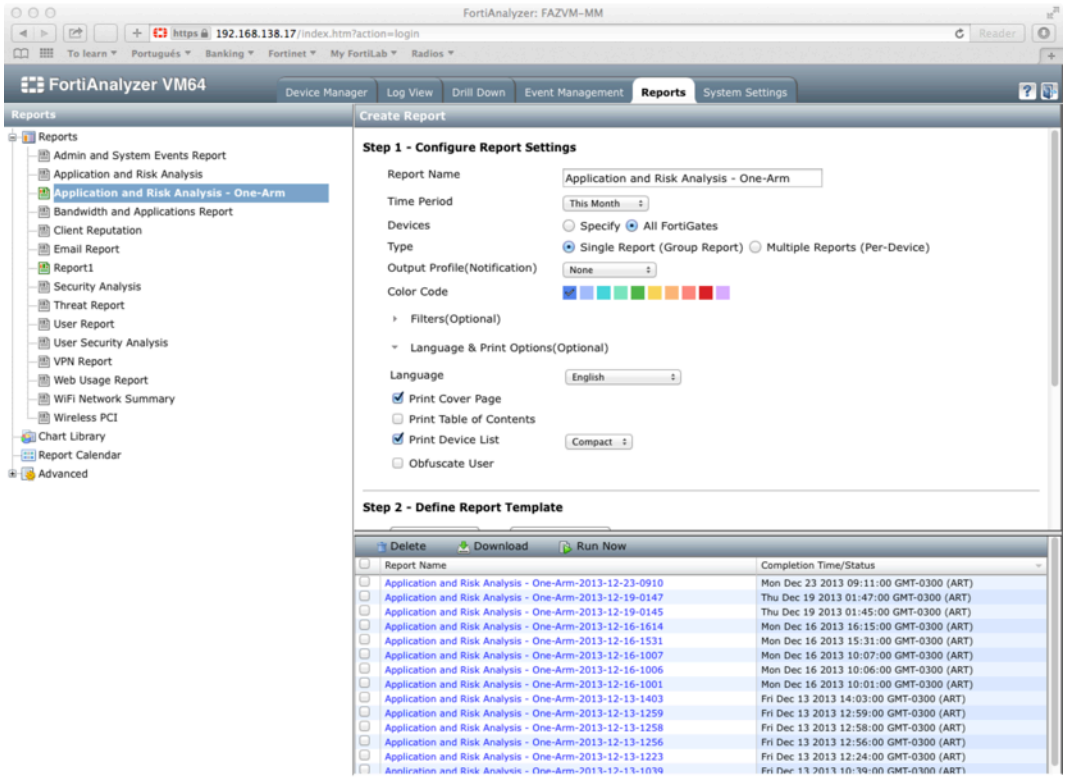
GUI

1. Go to Reports tab
2. Right click in any of the predefined reports and select “Import”

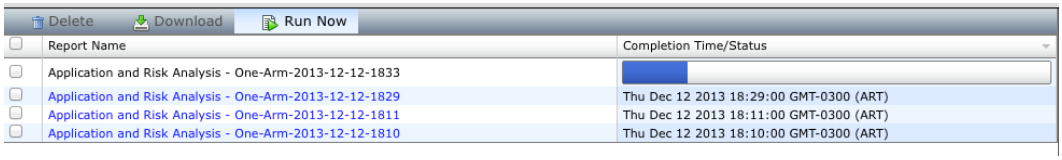


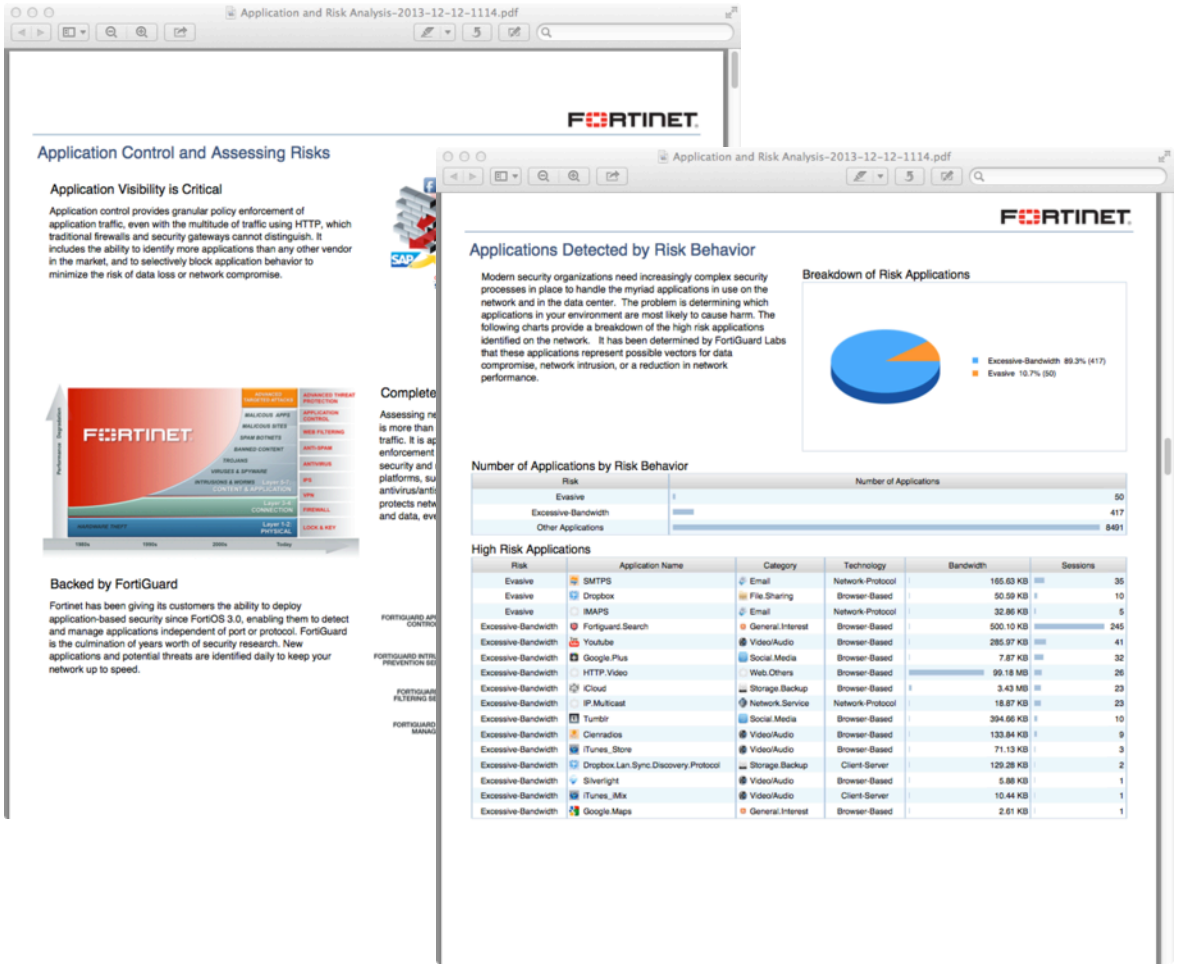

3. Search and select “Application and Risk Analysis – One Arm.dat” in the choose file dialog. Then click OK.
4. Once the report has been imported. Go to Reports → Application and Risk Analysis – One Arm
5. Select the “Time Period” of your choice according to the time the device has been collecting logs.
6. Devices: All FortiGates
7. Extend “Language & Print Options (Optional)”
8. Make sure “Print Cover Page” is enabled




9. Click Apply and then Run Now



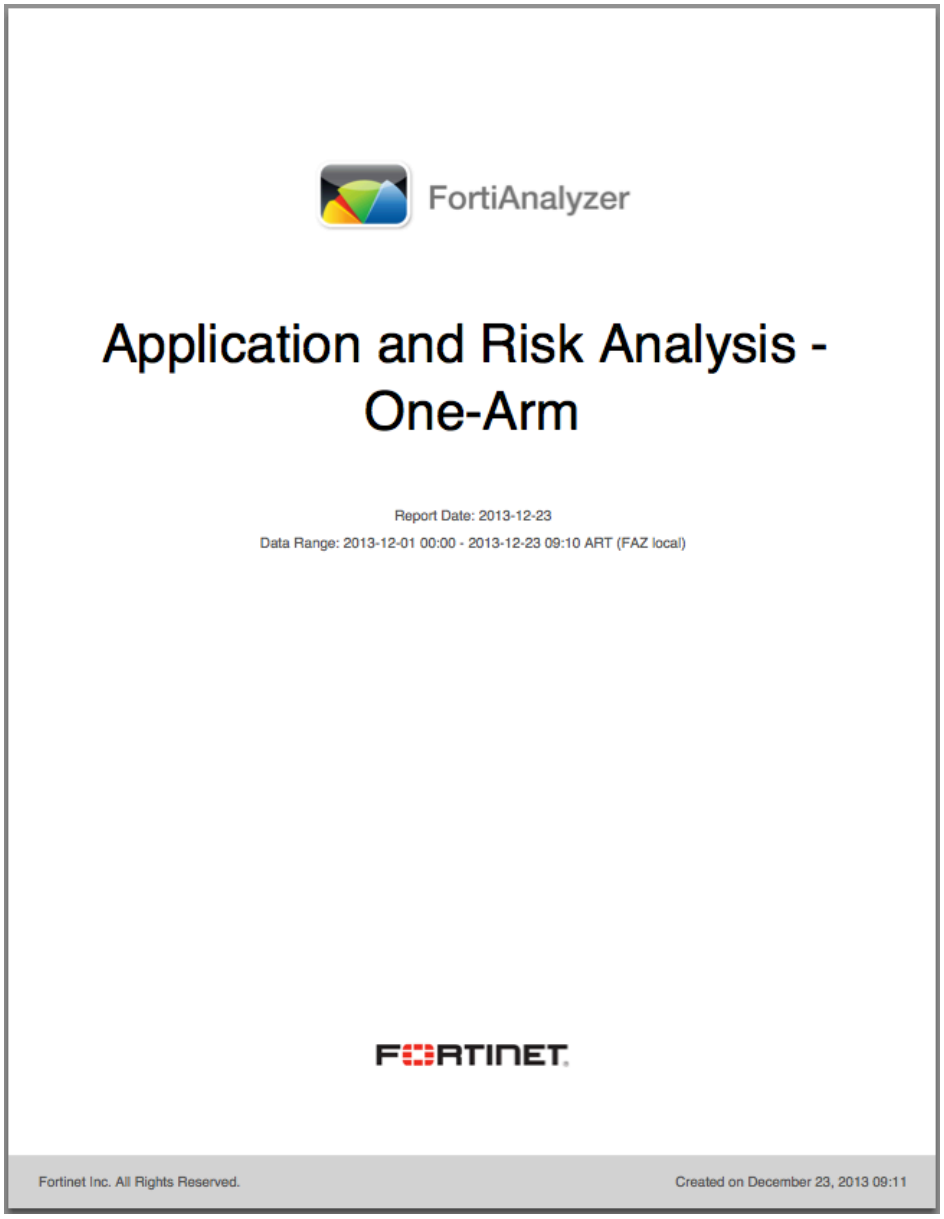

10. Wait until the reports has been generated and click on the report link to visualize it or choose the download button to get a PDF version of it
11. Analyze the generated report

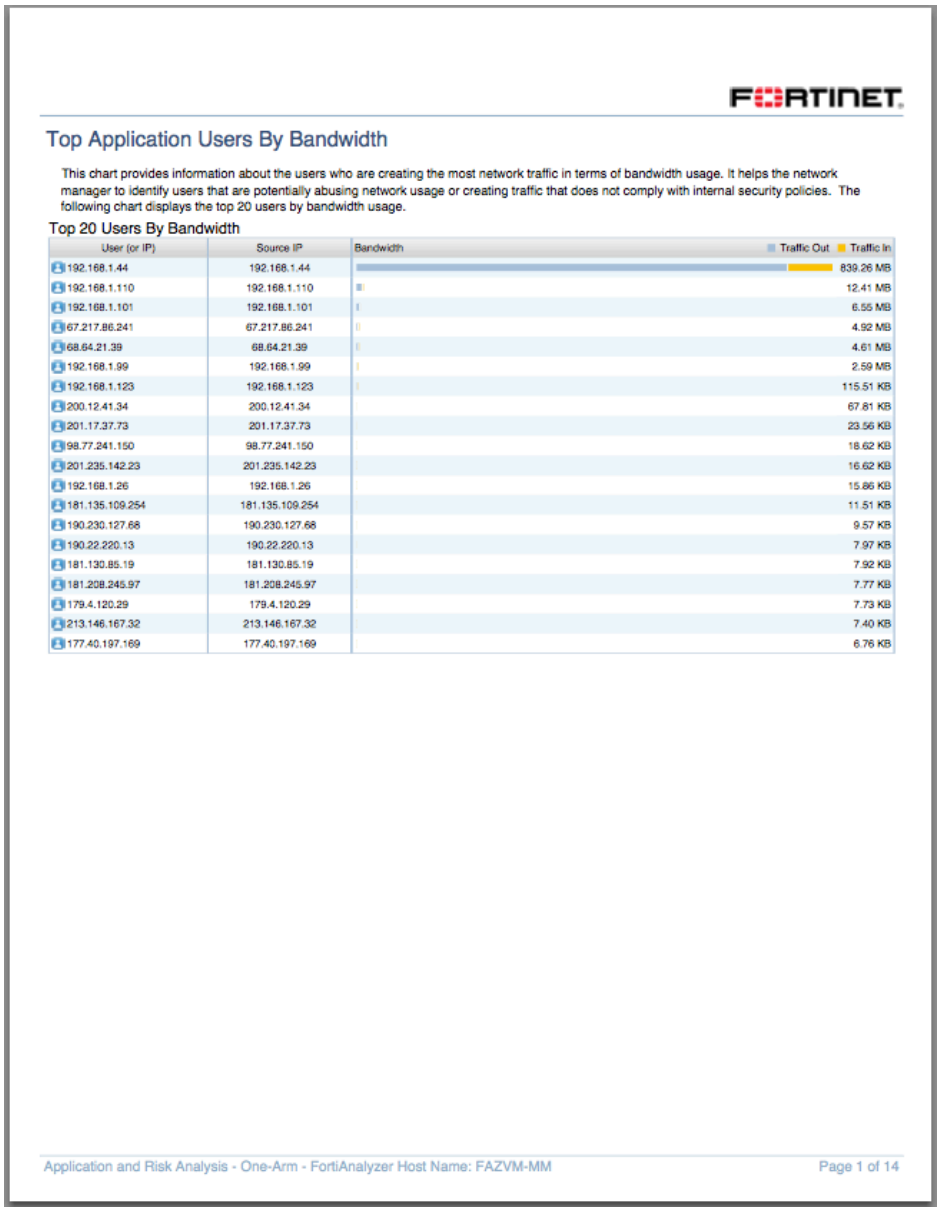

Application and Risk Analysis-2013-12-12-1114.pdf
Application Control and Assessing Risks
Application Visibility is Critical
Application control provides granular policy enforcement of application traffic, even with the multitude of traffic using HTTP, which traditional firewalls and security gateways cannot distinguish. It includes the ability to identify more applications than any other vendor in the market, and to selectively block application behavior to minimize the risk of data loss or network compromise.
Backed by FortiGuard
Fortinet has been giving its customers the ability to deploy application-based security since FortiOS 3.0, enabling them to detect and manage applications independent of port or protocol. FortiGuard is the culmination of years worth of security research. New applications and potential threats are identified daily to keep your network up to speed.
Application and Risk Analysis-2013-12-12-1114.pdf
Applications Detected by Risk Behavior
Modern security organizations need increasingly complex security processes in place to handle the myriad applications in use on the network and in the data center. The problem is determining which applications in your environment are most likely to cause harm. The following charts provide a breakdown of the high risk applications identified on the network. It has been determined by FortiGuard Labs that these applications represent possible vectors for data compromise, network intrusion, or a reduction in network performance.
Breakdown of Risk Applications
Excessive-Bandwidth 89.3% (417)
Evasive 10.7% (50)
Number of Applications by Risk Behavior
Risk
Number of Applications
Evasive 50
Excessive-Bandwidth 417
Other Applications 8491
High Risk Applications
Risk
Application Name
Category
Technology
Bandwidth
Sessions
Evasive SMTPS Email Network-Protocol 165.63 KB 35
Evasive Dropbox File.Sharing Browser-Based 50.59 KB 10
Evasive IMAPS Email Network-Protocol 32.86 KB 5
Excessive-Bandwidth Fortiguard.Search General.Interest Browser-Based 500.10 KB 245
Excessive-Bandwidth Youtube Video/Audio Browser-Based 285.97 KB 41
Excessive-Bandwidth Google.Plus Social.Media Browser-Based 7.87 KB 32
Excessive-Bandwidth HTTP.Video Web.Others Browser-Based 99.18 MB 26
Excessive-Bandwidth iCloud Storage.Backup Browser-Based 3.43 MB 23
Excessive-Bandwidth IP.Multicast Network.Service Network-Protocol 18.87 KB 23
Excessive-Bandwidth Tumblr Social.Media Browser-Based 394.66 KB 10
Excessive-Bandwidth Cienradios Video/Audio Browser-Based 133.84 KB 9
Excessive-Bandwidth iTunes_Store Video/Audio Browser-Based 71.13 KB 3
Excessive-Bandwidth Dropbox.Lan.Sync.Discovery.Protocol Storage.Backup Client-Server 129.28 KB 2
Excessive-Bandwidth Silverlight Video/Audio Browser-Based 5.88 KB 1
Excessive-Bandwidth iTunes_iMix Video/Audio Client-Server 10.44 KB 1
Excessive-Bandwidth Google.Maps General.Interest Browser-Based 2.61 KB 1

## APPLICATION AND RISK ANALYSIS REPORT – PRESENTATION TIPS

1. After reviewing the report make sure that there are no unpopulated charts, if some sections are blank due to no data customize the report to remove these sections
2. Do not email the ARA report to your customer. The report will have the most impact if you print it and share it with your customer in person. Keep in mind the report is very valuable and will often reveal new information about the customer's network.
3. Do your homework. Look through the report and determine problem areas starting with threats. Be prepared to make recommendations about application, web and bandwidth usage.
4. Use FortiGuard to research any anomalies that arise prior to your visit.

## APPENDIX I – SAMPLE REPORT





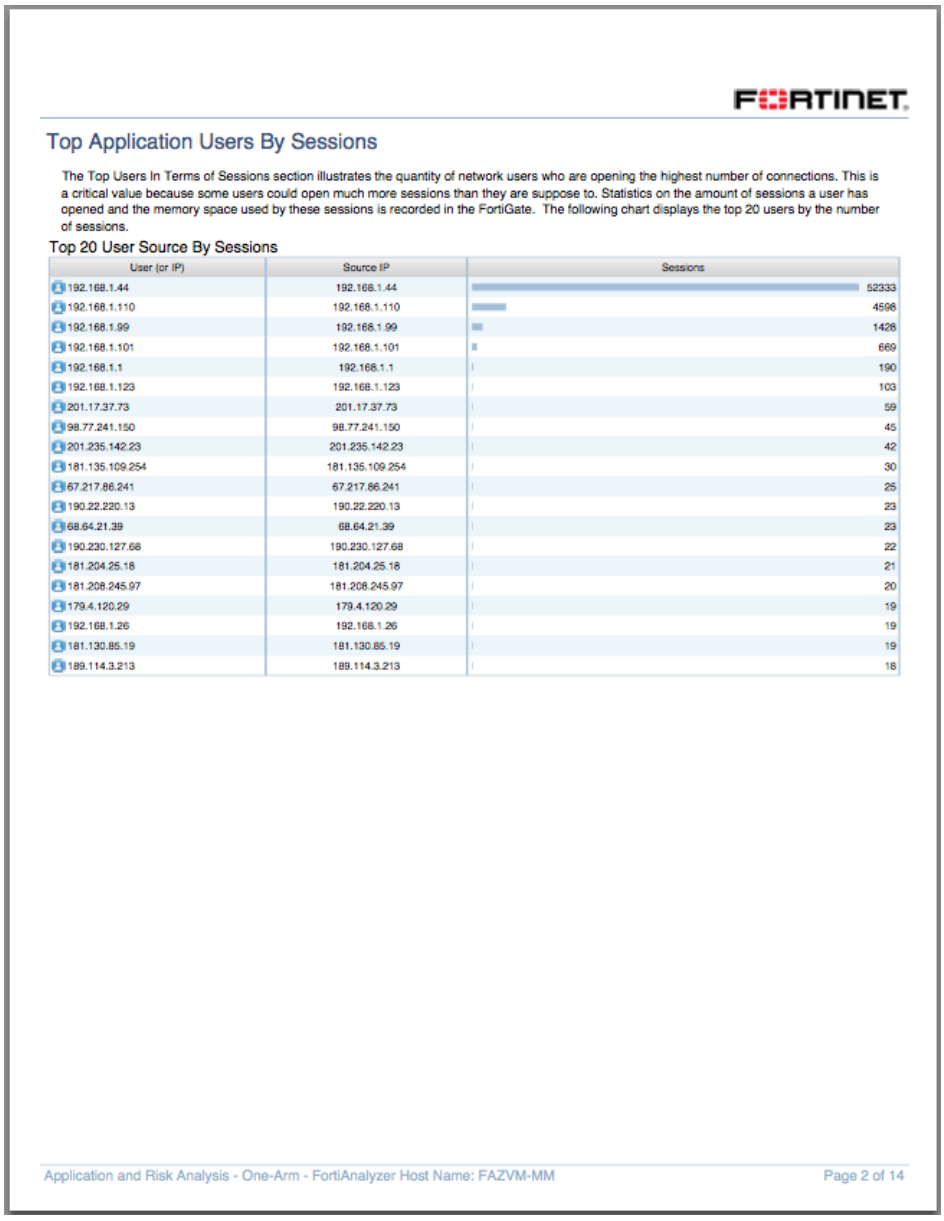
## Top Application Users By Bandwidth

This chart provides information about the users who are creating the most network traffic in terms of bandwidth usage. It helps the network manager to identify users that are potentially abusing network usage or creating traffic that does not comply with internal security policies. The following chart displays the top 20 users by bandwidth usage.

Top 20 Users By Bandwidth

| User (or IP) | Source IP | Bandwidth | Traffic Out | Traffic In |
|---|---|---|---|---|
| 192.168.1.44 | 192.168.1.44 | | | 839.26 MB |
| 192.168.1.110 | 192.168.1.110 | | | 12.41 MB |
| 192.168.1.101 | 192.168.1.101 | | | 6.55 MB |
| 67.217.86.241 | 67.217.86.241 | | | 4.92 MB |
| 68.64.21.39 | 68.64.21.39 | | | 4.61 MB |
| 192.168.1.99 | 192.168.1.99 | | | 2.59 MB |
| 192.168.1.123 | 192.168.1.123 | | | 115.51 KB |
| 200.12.41.34 | 200.12.41.34 | | | 67.81 KB |
| 201.17.37.73 | 201.17.37.73 | | | 23.56 KB |
| 98.77.241.150 | 98.77.241.150 | | | 18.62 KB |
| 201.235.142.23 | 201.235.142.23 | | | 16.62 KB |
| 192.168.1.26 | 192.168.1.26 | | | 15.86 KB |
| 181.135.109.254 | 181.135.109.254 | | | 11.51 KB |
| 190.230.127.68 | 190.230.127.68 | | | 9.57 KB |
| 190.22.220.13 | 190.22.220.13 | | | 7.97 KB |
| 181.130.85.19 | 181.130.85.19 | | | 7.92 KB |
| 181.208.245.97 | 181.208.245.97 | | | 7.77 KB |
| 179.4.120.29 | 179.4.120.29 | | | 7.73 KB |
| 213.146.167.32 | 213.146.167.32 | | | 7.40 KB |
| 177.40.197.169 | 177.40.197.169 | | | 6.76 KB |

Application and Risk Analysis - One-Arm - FortiAnalyzer Host Name: FAZVM-MM Page 1 of 14



## Top Application Users By Sessions

The Top Users In Terms of Sessions section illustrates the quantity of network users who are opening the highest number of connections. This is a critical value because some users could open much more sessions than they are suppose to. Statistics on the amount of sessions a user has opened and the memory space used by these sessions is recorded in the FortiGate. The following chart displays the top 20 users by the number of sessions.

Top 20 User Source By Sessions

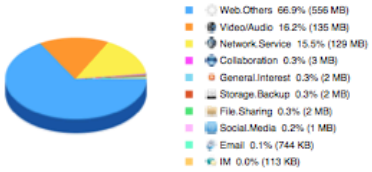
| User (or IP) | Source IP | Sessions |
|---|---|---|
| 192.168.1.44 | 192.168.1.44 | 52333 |
| 192.168.1.110 | 192.168.1.110 | 4598 |
| 192.168.1.99 | 192.168.1.99 | 1428 |
| 192.168.1.101 | 192.168.1.101 | 669 |
| 192.168.1.1 | 192.168.1.1 | 190 |
| 192.168.1.123 | 192.168.1.123 | 103 |
| 201.17.37.73 | 201.17.37.73 | 59 |
| 98.77.241.150 | 98.77.241.150 | 45 |
| 201.235.142.23 | 201.235.142.23 | 42 |
| 181.135.109.254 | 181.135.109.254 | 30 |
| 67.217.86.241 | 67.217.86.241 | 25 |
| 190.22.220.13 | 190.22.220.13 | 23 |
| 68.64.21.39 | 68.64.21.39 | 23 |
| 190.230.127.68 | 190.230.127.68 | 22 |
| 181.204.25.18 | 181.204.25.18 | 21 |
| 181.208.245.97 | 181.208.245.97 | 20 |
| 179.4.120.29 | 179.4.120.29 | 19 |
| 192.168.1.26 | 192.168.1.26 | 19 |
| 181.130.85.19 | 181.130.85.19 | 19 |
| 189.114.3.213 | 189.114.3.213 | 18 |

Application and Risk Analysis - One-Arm - FortiAnalyzer Host Name: FAZVM-MM Page 2 of 14

## Application Usage By Category

As part of the traffic classification process, the FortiGate identifies and categorizes the applications crossing the network into different categories based on the number of sessions and bandwidth. This data complements the granular application threat data and provides a more complete summary of the types of applications in use on the network.

Application Usage By Category




Top 30 Application Category

| Application Category | Bandwidth |
|---|---|
| Web.Others | 556.30 MB |
| Video/Audio | 134.82 MB |
| Network.Service | 128.53 MB |
| Collaboration | 2.72 MB |
| General.Interest | 2.41 MB |
| Storage.Backup | 2.12 MB |
| File.Sharing | 2.12 MB |
| Social.Media | 1.43 MB |
| Email | 743.87 KB |
| IM | 112.87 KB |
| Update | 99.11 KB |
| Remote.Access | 65.12 KB |

Application and Risk Analysis - One-Arm - FortiAnalyzer Host Name: FAZVM-MM Page 3 of 14

## Applications Detected by Risk Behavior

Modern security organizations need increasingly complex security processes in place to handle the myriad applications in use on the network and in the data center. The problem is determining which applications in your environment are most likely to cause harm. The following charts provide a breakdown of the high risk applications identified on the network. It has been determined by FortiGuard Labs that these applications represent possible vectors for data compromise, network intrusion, or a reduction in network performance.

### Breakdown of Risk Applications



### Number of Applications by Risk Behavior

| Risk | Number of Applications |
|---|---|
| Evasive | 731 |
| Excessive-Bandwidth | 1817 |
| Other Applications | 15097 |

### High Risk Applications

| Risk | Application Name | Category | Technology | Bandwidth | Sessions |
|---|---|---|---|---|---|
| Evasive | Twitter | Social.Media | Browser-Based | 1.04 MB | 562 |
| Evasive | SMTPS | Email | Network-Protocol | 550.96 KB | 111 |
| Evasive | Dropbox | File.Sharing | Browser-Based | 2.06 MB | 38 |
| Evasive | IMAPS | Email | Network-Protocol | 87.72 KB | 14 |
| Evasive | RTMP | Network.Service | Network-Protocol | 11.55 KB | 2 |
| Evasive | Gotomeeting | Collaboration | Browser-Based | 14.40 KB | 2 |
| Evasive | Stumbleupon.Toolbar | General.Interest | Browser-Based | 1.57 KB | 1 |
| Evasive | Jabber | IM | Client-Server | 112.67 KB | 1 |
| Excessive-Bandwidth | Fortiguard.Search | General.Interest | Browser-Based | 1.98 MB | 1.11 K |
| Excessive-Bandwidth | iCloud | Storage.Backup | Browser-Based | 2.03 MB | 181 |
| Excessive-Bandwidth | Youtube | Video/Audio | Browser-Based | 2.25 MB | 135 |
| Excessive-Bandwidth | iTunes | Video/Audio | Client-Server | 8.17 MB | 126 |
| Excessive-Bandwidth | IP.Multicast | Network.Service | Network-Protocol | 36.06 KB | 60 |
| Excessive-Bandwidth | HTTP.Video | Web.Others | Browser-Based | 147.49 MB | 54 |
| Excessive-Bandwidth | Youtube_HD.Streaming | Video/Audio | Browser-Based | 123.07 MB | 40 |
| Excessive-Bandwidth | Akamai | File.Sharing | Browser-Based | 4.91 KB | 32 |
| Excessive-Bandwidth | iTunes_Store | Video/Audio | Browser-Based | 955.83 KB | 25 |
| Excessive-Bandwidth | Google.Plus | Social.Media | Browser-Based | 4.67 KB | 19 |
| Excessive-Bandwidth | Cienradios | Video/Audio | Browser-Based | 346.13 KB | 13 |
| Excessive-Bandwidth | HTTP.Audio | Web.Others | Browser-Based | 18.93 MB | 10 |

## Key Applications Crossing The Network

This part of the PoC Security Report offers a summary of the key applications crossing the network based on the amount of bandwidth they are using and then sorted into different application types. It provides a high level view of the types of application that are used most commonly across the network.

### Key Applications Crossing The Network

| Application | Category | Sessions | Bandwidth |
|---|---|---|---|
| HTTP.BROWSER_Safari | Web.Others | 2138 | 341.39 MB |
| HTTP.Video | Web.Others | 54 | 147.49 MB |
| SSL | Network.Service | 7575 | 127.22 MB |
| Youtube_HD.Streaming | Video/Audio | 40 | 123.07 MB |
| HTTP.BROWSER | Web.Others | 239 | 27.13 MB |
| HTTP.Audio | Web.Others | 10 | 18.93 MB |
| HTTP.Flash | Web.Others | 3 | 16.86 MB |
| Web Management(HTTPS) | | 108 | 13.03 MB |
| iTunes | Video/Audio | 126 | 8.17 MB |
| HTTP.BROWSER_Firefox | Web.Others | 115 | 3.52 MB |
| Zoho | Collaboration | 73 | 2.69 MB |
| Youtube | Video/Audio | 135 | 2.25 MB |
| Dropbox | File.Sharing | 38 | 2.06 MB |
| iCloud | Storage.Backup | 181 | 2.03 MB |
| Fortiguard.Search | General.Interest | 1109 | 1.98 MB |
| Twitter | Social.Media | 562 | 1.04 MB |
| iTunes_Store | Video/Audio | 25 | 955.83 KB |
| DNS | Network.Service | 3881 | 708.52 KB |
| SMTPS | Email | 111 | 550.96 KB |
| Console Management(SSH) | | 3 | 519.40 KB |
| Geckoboard | Web.Others | 12 | 515.99 KB |
| Salesforce | General.Interest | 12 | 411.04 KB |
| Facebook | Social.Media | 26 | 372.03 KB |
| Cienradios | Video/Audio | 13 | 346.13 KB |
| ICMP | Network.Service | 685 | 287.19 KB |
| HTTP.BROWSER_IE | Web.Others | 18 | 268.43 KB |
| OCSP | Network.Service | 96 | 210.62 KB |
| HTTP.PDF | Web.Others | 1 | 198.32 KB |
| Jabber | IM | 1 | 112.87 KB |
| Gmail | Email | 8 | 105.19 KB |

Application and Risk Analysis - One-Arm - FortiAnalyzer Host Name: FAZVM-MM Page 5 of 14

## Applications Running Over HTTP

This section provides an overview of applications crossing the network that use HTTP. Software updates, error reporting or help guides are used by different business applications as a means of improving the overall user experience. Social networks, streaming video or audio, file sharing are among the most common non-business applications that use HTTP. Assessing the number and type of applications that use HTTP provides a critical part of developing an efficient network security strategy.

Applications Running Over HTTP

| Application | Sessions | Bandwidth |
|---|---|---|
| HTTP.BROWSER_Safari | 2137 | 341.39 MB |
| HTTP.Video | 54 | 147.49 MB |
| SSL | 7532 | 125.90 MB |
| Youtube_HD.Streaming | 40 | 123.07 MB |
| HTTP.BROWSER | 238 | 27.13 MB |
| HTTP.Audio | 10 | 18.93 MB |
| HTTP.Flash | 3 | 16.86 MB |
| Web Management(HTTPS) | 108 | 13.03 MB |
| iTunes | 126 | 8.17 MB |
| HTTP.BROWSER_Firefox | 115 | 3.52 MB |
| Youtube | 126 | 2.20 MB |
| Zoho | 49 | 2.13 MB |
| iCloud | 181 | 2.03 MB |
| Dropbox | 37 | 1.85 MB |
| Twitter | 554 | 984.91 KB |
| iTunes_Store | 25 | 955.83 KB |
| Zoho | 24 | 555.74 KB |
| Geckoboard | 12 | 515.99 KB |
| Salesforce | 12 | 411.04 KB |
| Facebook | 20 | 349.85 KB |
| Cienradios | 13 | 346.13 KB |
| HTTP.BROWSER_IE | 18 | 268.43 KB |
| OCSP | 96 | 210.62 KB |
| Dropbox | 1 | 204.93 KB |
| HTTP.PDF | 1 | 198.32 KB |

Application and Risk Analysis - One-Arm - FortiAnalyzer Host Name: FAZVM-MM Page 6 of 14

## Top Web Categories Visited By Network Users

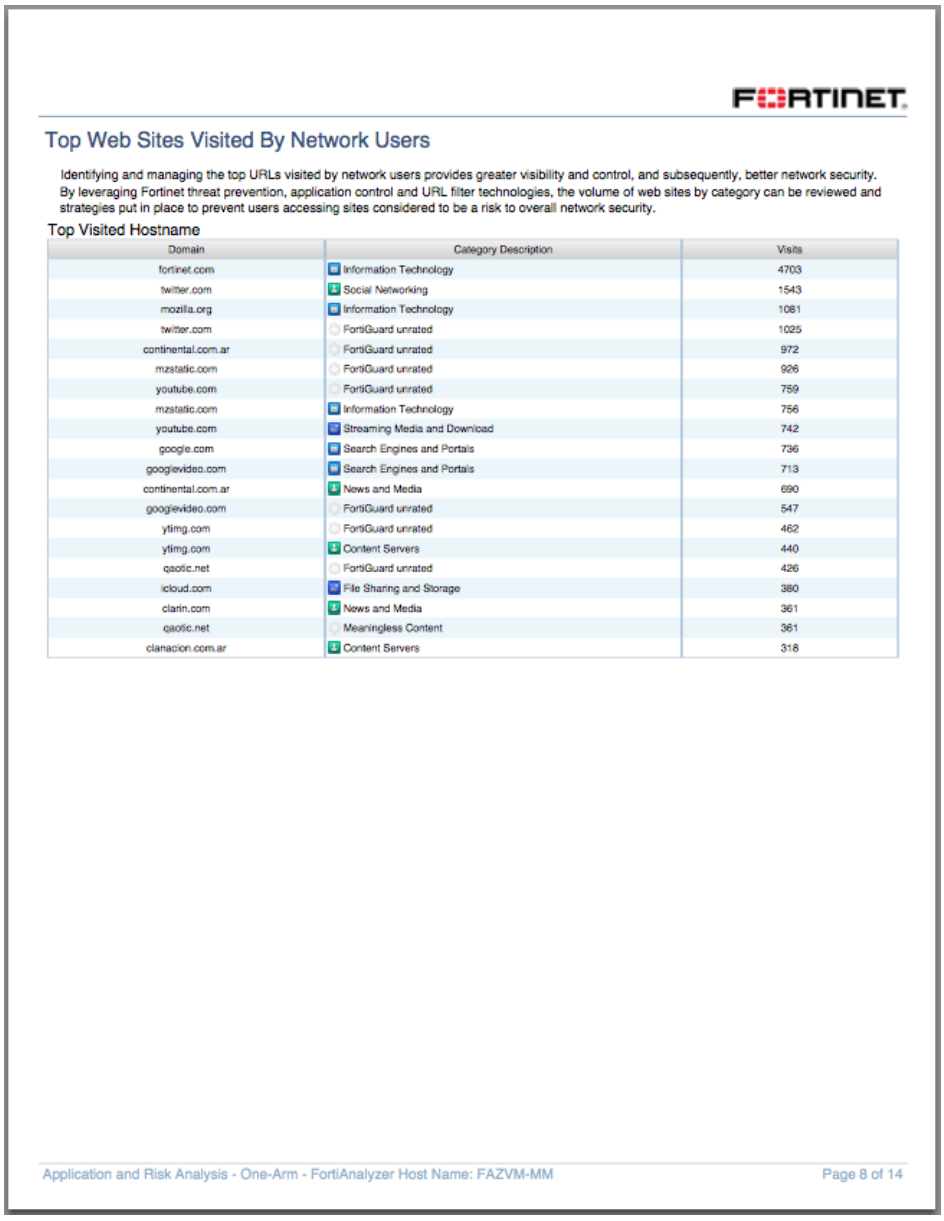
User browsing habits can not only be indicative of inefficient use of corporate resources, but can also indicate an inefficient optimization of web filtering policies. It can also give some insight into the general web browsing habits of corporate users and assist in defining corporate compliance guidelines. This chart details web categories by the number of times URLs within those categories were requested and by the number of bandwidth used.

Top Web Categories


Top Web Sites Visited By Network Users

| Category Description | Sessions | Bandwidth |
|---|---|---|
| Information Technology | 8229 | 6.55 MB |
| FortiGuard unrated | 8067 | 615.36 MB |
| Social Networking | 1738 | 967.75 KB |
| Search Engines and Portals | 1717 | 2.98 MB |
| News and Media | 1326 | 3.95 MB |
| Content Servers | 991 | 711.89 KB |
| Streaming Media and Download | 865 | 1.29 MB |
| File Sharing and Storage | 647 | 989.90 KB |
| Advertising | 547 | 681.68 KB |
| Meaningless Content | 369 | 158.03 KB |
| Internet Radio and TV | 182 | 75.02 KB |
| Web-based Email | 75 | 177.04 KB |
| Business | 74 | 57.34 KB |
| Reference | 72 | 92.86 KB |
| Web-based Applications | 55 | 36.51 KB |
| Travel | 35 | 27.03 KB |
| Internet Telephony | 26 | 82.00 KB |
| Finance and Banking | 22 | 44.47 KB |
| Illegal or Unethical | 21 | 10.46 KB |
| Web Hosting | 16 | 3.09 KB |

Application and Risk Analysis - One-Arm - FortiAnalyzer Host Name: FAZVM-MM Page 7 of 14



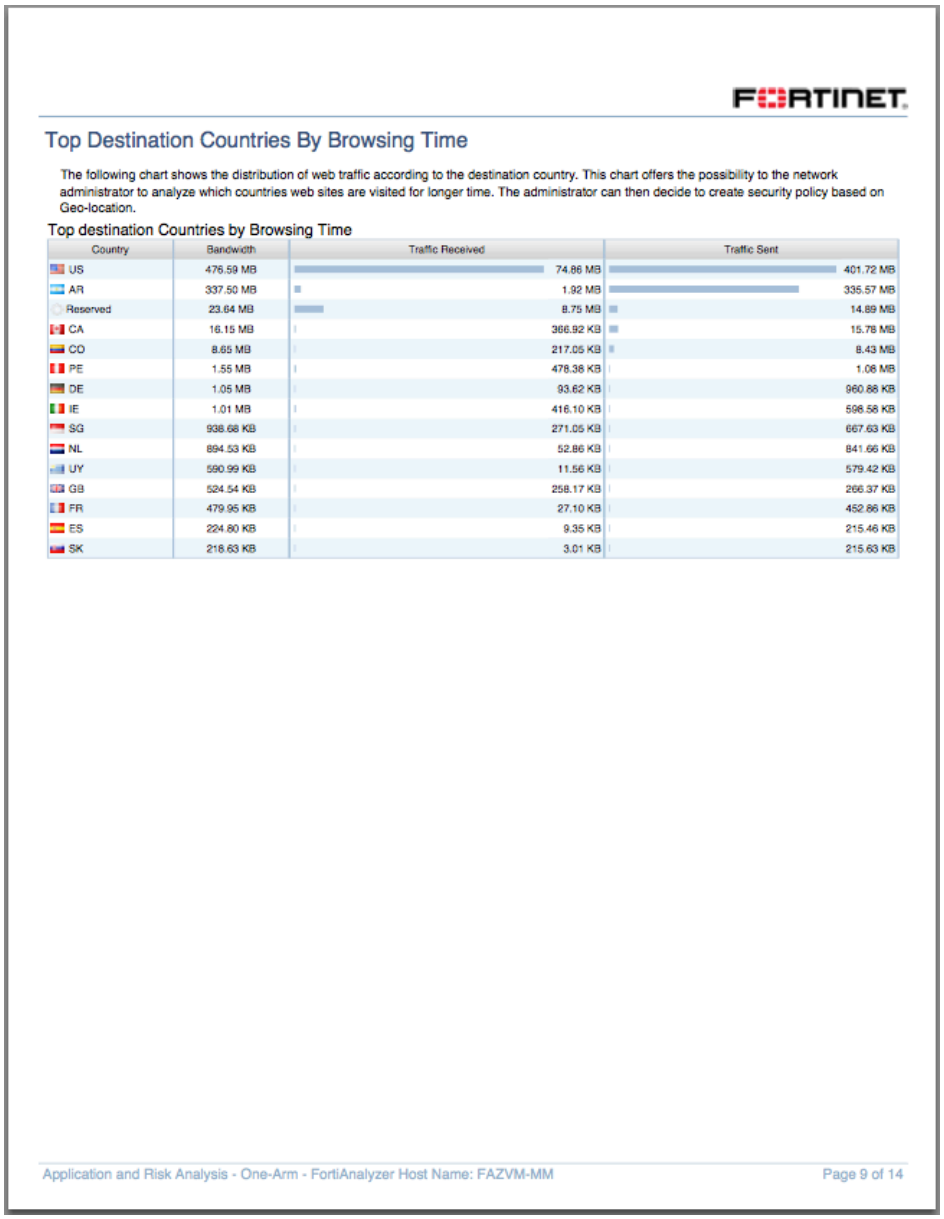
## Top Web Sites Visited By Network Users

Identifying and managing the top URLs visited by network users provides greater visibility and control, and subsequently, better network security. By leveraging Fortinet threat prevention, application control and URL filter technologies, the volume of web sites by category can be reviewed and strategies put in place to prevent users accessing sites considered to be a risk to overall network security.

Top Visited Hostname

| Domain | Category Description | Visits |
|---|---|---|
| fortinet.com | Information Technology | 4703 |
| twitter.com | Social Networking | 1543 |
| mozilla.org | Information Technology | 1081 |
| twitter.com | FortiGuard unrated | 1025 |
| continental.com.ar | FortiGuard unrated | 972 |
| mzstatic.com | FortiGuard unrated | 926 |
| youtube.com | FortiGuard unrated | 759 |
| mzstatic.com | Information Technology | 756 |
| youtube.com | Streaming Media and Download | 742 |
| google.com | Search Engines and Portals | 736 |
| googlevideo.com | Search Engines and Portals | 713 |
| continental.com.ar | News and Media | 690 |
| googlevideo.com | FortiGuard unrated | 547 |
| ytimg.com | FortiGuard unrated | 462 |
| ytimg.com | Content Servers | 440 |
| qaotic.net | FortiGuard unrated | 426 |
| icloud.com | File Sharing and Storage | 380 |
| clarin.com | News and Media | 361 |
| qaotic.net | Meaningless Content | 361 |
| clanacion.com.ar | Content Servers | 318 |

Application and Risk Analysis - One-Arm - FortiAnalyzer Host Name: FAZVM-MM Page 8 of 14



## Top Destination Countries By Browsing Time

The following chart shows the distribution of web traffic according to the destination country. This chart offers the possibility to the network administrator to analyze which countries web sites are visited for longer time. The administrator can then decide to create security policy based on Geo-location.

Top destination Countries by Browsing Time

| Country | Bandwidth | Traffic Received | Traffic Sent |
|---|---|---|---|
| US | 476.59 MB | 74.86 MB | 401.72 MB |
| AR | 337.50 MB | 1.92 MB | 335.57 MB |
| Reserved | 23.64 MB | 8.75 MB | 14.89 MB |
| CA | 16.15 MB | 366.92 KB | 15.78 MB |
| CO | 8.65 MB | 217.05 KB | 8.43 MB |
| PE | 1.55 MB | 478.38 KB | 1.08 MB |
| DE | 1.05 MB | 93.62 KB | 960.88 KB |
| IE | 1.01 MB | 416.10 KB | 598.58 KB |
| SG | 938.68 KB | 271.05 KB | 667.63 KB |
| NL | 894.53 KB | 52.86 KB | 841.66 KB |
| UY | 590.99 KB | 11.56 KB | 579.42 KB |
| GB | 524.54 KB | 258.17 KB | 266.37 KB |
| FR | 479.95 KB | 27.10 KB | 452.86 KB |
| ES | 224.80 KB | 9.35 KB | 215.46 KB |
| SK | 218.63 KB | 3.01 KB | 215.63 KB |

Application and Risk Analysis - One-Arm - FortiAnalyzer Host Name: FAZVM-MM Page 9 of 14

## Top Threats Crossing The Network

By individually reviewing both the applications and traffic flows crossing the network, threat vector identification and prevention becomes easier. Threat prevention technologies filter the total number of applications and traffic crossing the network down to those applications or packets that pose a potential risk, picking up threat vectors such as spyware, application vulnerabilities or viruses. The result is improved overall network performance and lower network latency.

Top Threat Vectors Crossing The Network


Top Critical Threat Vectors Crossing The Network

| Attack Name | Reference | Total Num |
|---|---|---|
| Cisco.IOS.HTTP.Remote.Command.Execution | http://www.fortinet.com/ids/VID30478 | 1 |

Top High Threat Vectors Crossing The Network

| Attack Name | Reference | Total Num |
|---|---|---|
| Cisco.CSCdv50135.Telnet.Buffer.Overflow | http://www.fortinet.com/ids/VID32370 | 89 |

Top Medium Threat Vectors Crossing The Network

| Attack Name | Reference | Total Num |
|---|---|---|
| Cisco.514.UDP.Flood.DoS | http://www.fortinet.com/ids/VID32375 | 3 |
| Cisco.600.Series.Web.Administration.DoS | http://www.fortinet.com/ids/VID32374 | 1 |
| Cisco.UTF.Encoding.IDS.Bypass | http://www.fortinet.com/ids/VID32373 | 1 |
| Cisco.CatOS.CiscoView.HTTP.Server.Buffer.Overflow | http://www.fortinet.com/ids/VID32372 | 1 |
| Cisco.IOS.HTTP.Server.Query.DoS | http://www.fortinet.com/ids/VID32376 | 1 |

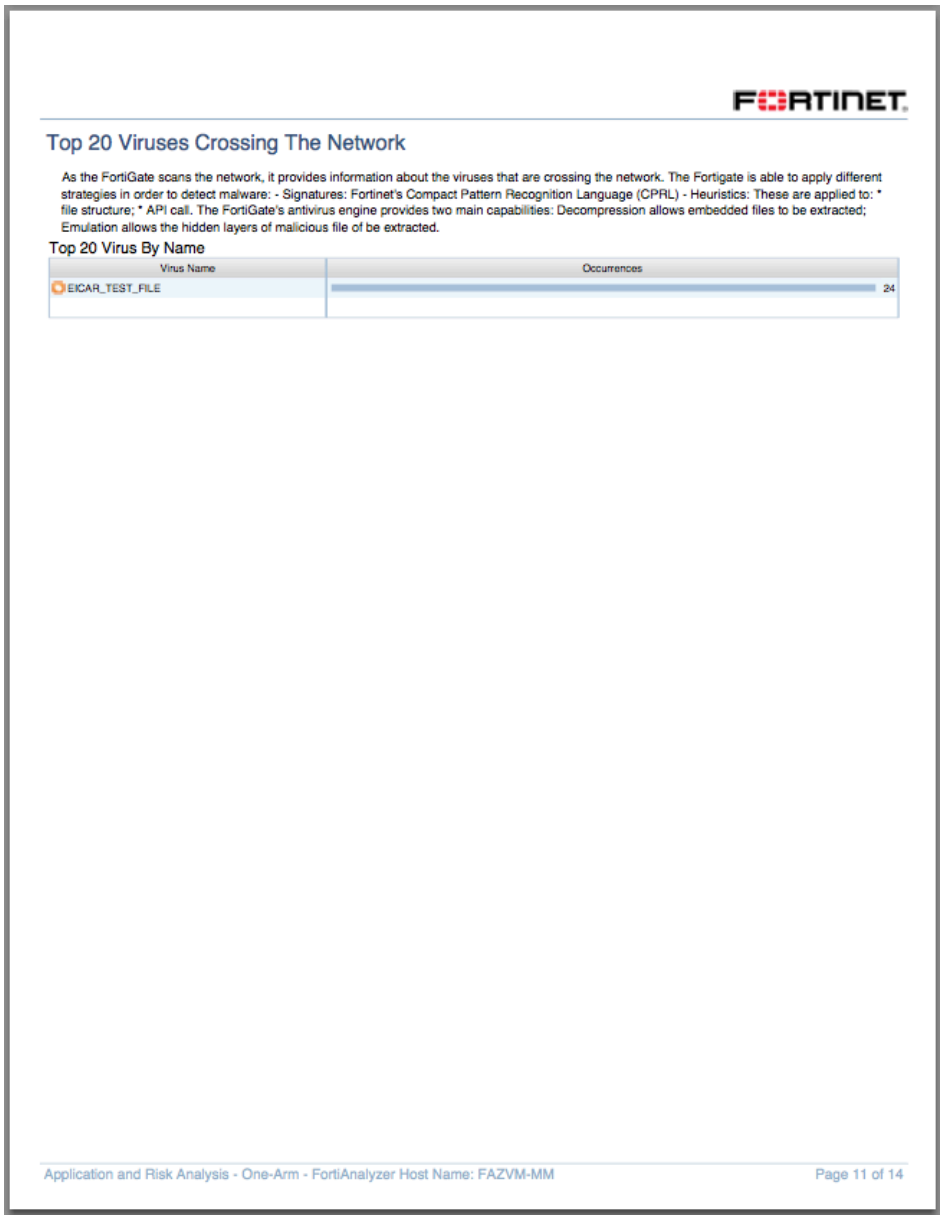
Top Low Threat Vectors Crossing The Network

No matching log data for this report

Top Info Threat Vectors Crossing The Network

No matching log data for this report

Application and Risk Analysis - One-Arm - FortiAnalyzer Host Name: FAZVM-MM Page 10 of 14



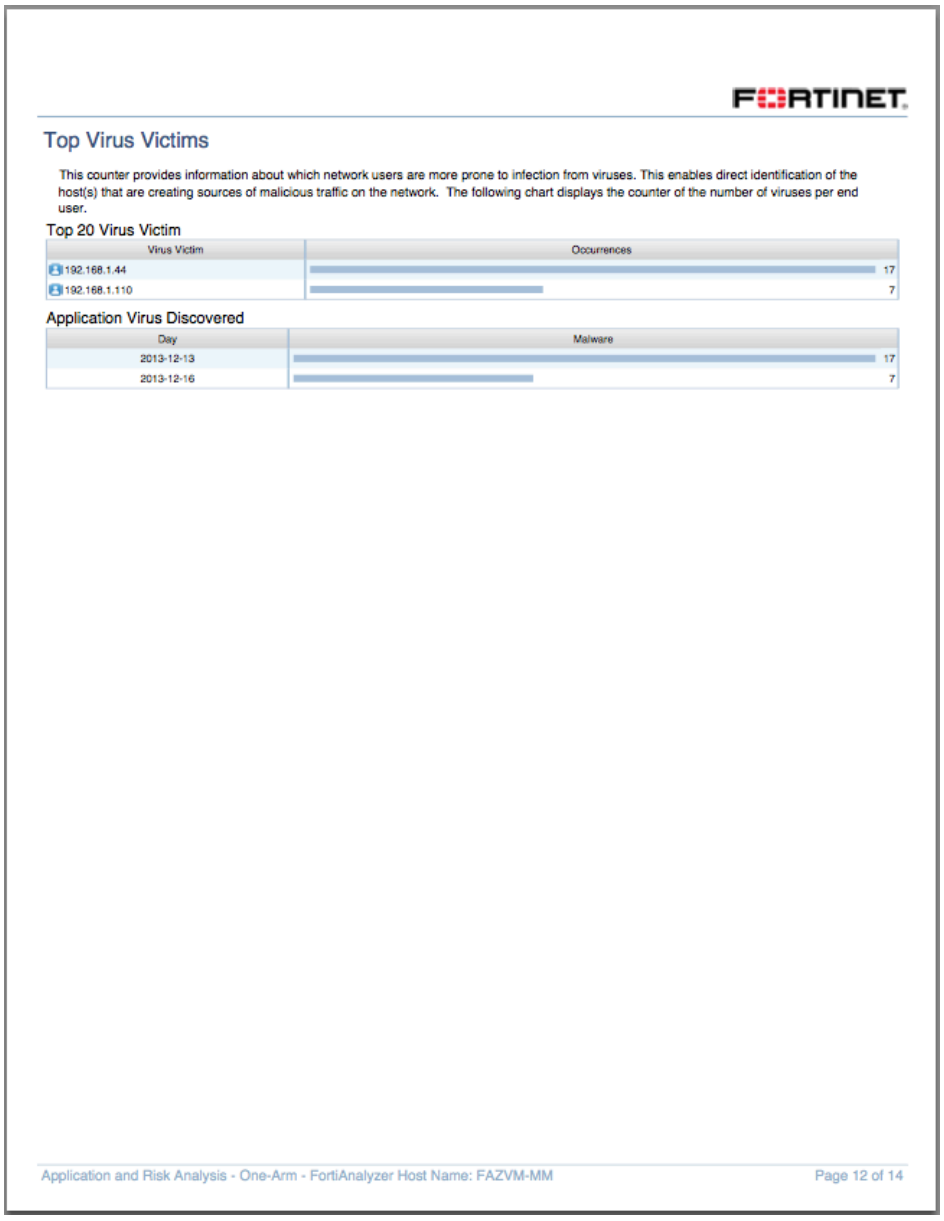
## Top 20 Viruses Crossing The Network

As the FortiGate scans the network, it provides information about the viruses that are crossing the network. The Fortigate is able to apply different strategies in order to detect malware: - Signatures: Fortinet's Compact Pattern Recognition Language (CPRL) - Heuristics: These are applied to: * file structure; * API call. The FortiGate's antivirus engine provides two main capabilities: Decompression allows embedded files to be extracted; Emulation allows the hidden layers of malicious file of be extracted.

Top 20 Virus By Name

| Virus Name | Occurrences |
|---|---|
| EICAR_TEST_FILE | 24 |

Application and Risk Analysis - One-Arm - FortiAnalyzer Host Name: FAZVM-MM Page 11 of 14



## Top Virus Victims

This counter provides information about which network users are more prone to infection from viruses. This enables direct identification of the host(s) that are creating sources of malicious traffic on the network. The following chart displays the counter of the number of viruses per end user.

Top 20 Virus Victim

| Virus Victim | Occurrences |
|---|---|
| 192.168.1.44 | 17 |
| 192.168.1.110 | 7 |

Application Virus Discovered

| Day | Malware |
|---|---|
| 2013-12-13 | 17 |
| 2013-12-16 | 7 |

Application and Risk Analysis - One-Arm - FortiAnalyzer Host Name: FAZVM-MM Page 12 of 14

# APPENDIX II – SNIFFER MODE – POC CHECK LIST

### STEP ZERO

- ☐ Do all this procedure on a controlled network (your own company network!) at least once before attempting this on a customer's network.

### BEFORE DOING ANY CONFIGURATION

- ☐ Call the customer. Gather every information you will need during the POC
- ☐ Make sure products are registered, with valid FortiGuard contracts and proper FortiOS versions.
- ☐ Make sure paperwork has been done and that you won't have any logistic issue to get the equipment inserted into the customer's network

### CONFIGURING THE FORTIGATE

- ☐ Do a factory reset
- ☐ Configure networking: Management interface, DNS, default gateway and other routes. Test your networking configuration
- ☐ Update FortiGuard signatures and engines
- ☐ Configure sniffing interface
- ☐ Configure security profiles: Antivirus, Application Control, Web Filtering, IPS
- ☐ Configure sniffing policy

## CONFIGURING THE FORTIANALYZER

- ☐ Setup FortiAnalyzer
- ☐ Configure FortiGate to send logs to FortiAnalyzer
- ☐ Setup networking (switch, router) so traffic gets copied to FortiGate.
- ☐ Verify that the FortiGate is receiving network traffic
- ☐ Review logs and generate reports
- ☐ Provide customer with generated reports
- ☐ Make sure you provide a follow-up email/report summarizing the results of the POC.
- ☐ Sell!

## APPENDIX III – REFERENCES

- CLI Reference Guide for FortiOS 5.0
  http://docs.fortinet.com/fgt/handbook/50/5-0-4/fortigate-cli-50.pdf

- Install and System Administration for FortiOS 5.0
  http://docs.fortinet.com/fgt/handbook/50/5-0-4/fortigate-install-system-admin-50.pdf

- Security Profiles for FortiOS 5.0
  http://docs.fortinet.com/fgt/handbook/50/fortigate-security_profiles-50.pdf

- The FortiOS Handbook
  http://docs.fortinet.com/fgt/handbook/50/fortios-handbook-50.pdf

- FortiAnalyzer v5.0 Administration Guide
  http://docs.fortinet.com/fa/50/FortiAnalyzer-504-Admin-Guide.pdf

- The FortiGate Cookbook
  http://docs.fortinet.com/cookbook.html

- FortiGuard Center
  http://www.fortiguard.com